

1 UNITED STATES DISTRICT COURT
2 FOR THE NORTHERN DISTRICT OF OHIO
3 EASTERN DIVISION

4 - - - - -

5 UNITED STATES OF AMERICA,)
6 Plaintiff,)
7 vs.) Case No. 1:16CR224
8 BOGDAN NICOLESCU,)
9 RADU MICLAUS,)
10 Defendants.)

11 - - - - -

12
13 CONTINUED TRANSCRIPT OF TRIAL PROCEEDINGS HAD
14 BEFORE HONORABLE JUDGE PATRICIA A. GAUGHAN, JUDGE
15 OF SAID COURT, ON TUESDAY, APRIL 2ND, 2019,
16 COMMENCING AT 9:00 O'CLOCK A.M.

17 - - - - -

18 Volume 7, Pages 1146 through 1378
19 - - - - -

20
21
22
23 Court Reporter: GEORGE J. STAUDUHAR
24 801 W. SUPERIOR AVE.,
25 SUITE 7-184
CLEVELAND, OHIO 44113
(216) 357-7128

1 APPEARANCES:

2 On behalf of the Government:

3 OFFICE OF THE U.S. ATTORNEY
4 BY: DUNCAN T. BROWN, AUSA
5 BRIAN M. McDONOUGH, AUSA
6 801 West Superior Ave., Suite 400
7 Cleveland, OH 44113

8 and

9 U.S. DEPARTMENT OF JUSTICE - CRIMINAL DIVISION
10 BY: BRIAN L. LEVINE, SENIOR COUNSEL
11 1301 New York Avenue, Suite 600
12 Washington, DC 20530

13 On behalf of Defendant Bogdan Nicolescu:

14 LAW OFFICE OF MICHAEL J. GOLDBERG
15 BY: MICHAEL J. GOLDBERG, ESQ.
16 323 Lakeside Place, Suite 450
17 Cleveland, OH 44113

18 On behalf of Defendant Radu Miclaus:

19 LIPSON O'SHEA
20 BY: MICHAEL J. O'SHEA, ESQ.
21 110 Hoyt Block Building
22 700 West St. Clair Avenue
23 Cleveland, OH 44113
24
25

I N D E X

<u>WITNESSES:</u>	<u>DIRECT</u>	<u>CROSS</u>	<u>REDIRECT</u>	<u>RECROSS</u>
Amber Leavitt	1194			
By Mr. Goldberg		1164		
By Mr. O'Shea		1166		
Matthew Frost	1172			
By Mr. Goldberg		1209		
By Mr. O'Shea		1378		
Tiberiu Danet	1242			

Ms. Leavitt - Direct

P R O C E E D I N G S

THE COURT: Okay. Call your next witness.

MR. McDONOUGH: United States of America
would call Amber Leavitt.

Please step up to the podium, Ma'am. Please
raise your right hand.

AMBER LEAVITT

called as a witness by and on behalf of the Government,
being first duly sworn, was examined and testified
as follows:

THE COURT: Please take a seat right over
there.

DIRECT EXAMINATION

BY MR. McDONOUGH:

Q. Good morning. Could you please state your name, and
spell your last name for the benefit of our court
reporter?

A. Yes. It is Amber Leavitt, A-m-b-e-r, L-e-a-v-i-t-t.

Q. By whom are you employed?

A. EBay, Inc.

Q. In what capacity?

A. I am employed as an attorney.

My official title is senior director of
global intellectual property.

Q. How long have you been senior director of

Ms. Leavitt - Direct

1 intellectual property at eBay?

2 A. For about three years.

3 Q. What are your duties and responsibilities as senior
4 director of intellectual property?

5 A. So I oversee management of the trademark and domain
6 portfolios for the company, and I also oversee our
7 anticounterfeiting and antiinfringement policies, and I
8 also am responsible for management of our verified rights
9 owner or VeRO program.

10 Q. Okay. How many trademark attorneys does eBay
11 have?

12 A. You are looking at her.

13 Q. Okay. Do you have any support staff?

14 A. I do have one trademark paralegal.

15 Q. Okay. You mentioned intellectual property. What's
16 intellectual property?

17 A. The way I would describe intellectual property is
18 inventions of the mind.

19 Q. You mentioned you oversee trademark and domain
20 portfolios.

21 What are those?

22 A. So the trademark portfolio is essentially a set of
23 trademarks that help us to identify our products and
24 services, and as part of that, I help to register those
25 marks and then enforce them against people who are using

Ms. Leavitt - Direct

1 them without authorization.

2 Q. Okay. How many trademarks does eBay have?

3 A. Currently, we have around 1,400, either registered
4 or pending applications.

5 Q. Okay. You mentioned something about
6 anticounterfeiting policies and processes. What can did
7 you mean by that?

8 A. So those are basically the different things that we
9 do to try to prevent fake products from showing up on our
10 site.

11 So I think a good example is like a fake
12 purse or shoes. We try to work to make sure those things
13 don't end up on the site in the first place.

14 Q. And you mentioned the administration of verified
15 rights program. What was that?

16 A. Yes. So the verified rights program is a notice and
17 takedown program, so if a brand, say Nike, sees that
18 there is a product on our site like a fake shoe, they can
19 use that program to report that as infringing their
20 intellectual property rights.

21 Q. Is it Nike's responsibility to check through all the
22 eBay ads, or is it eBay's or both or none or —

23 A. It is kind of an ecosystem, right?

24 So it is in our interest to prevent those
25 types of items from showing up on the site, so we do

Ms. Leavitt - Direct

1 various things to try to identify and then remove those
2 types of products?

3 But then, that's where we kind of partner
4 with rights owners, is we rely on them to help us
5 identify things that we might not otherwise know are
6 problematic.

7 Q. Ecosystem is — what's that again, ecosystem?

8 A. So it is kind of a cooperative relationship is how I
9 would describe it.

10 Q. And eBay has partners?

11 A. What do you mean by partners?

12 Q. You mentioned in order for eBay's trademarks, do you
13 have to give permission to someone to go ahead and use
14 them?

15 A. Yes, that's correct.

16 Q. So you have partnerships or do you enter into — you
17 have partners when it comes to giving permission to use
18 the eBay trademarks?

19 A. Yes. We will license use of our marks and most
20 commonly it is for a business relationship or
21 partnership.

22 Q. Can you give an example of eBay giving a license to
23 use the eBay trademark to another company?

24 A. Yes. I think one of the most recent examples is the
25 "Wreck-It Ralph 2" movie, the recent Disney movie. EBay

Ms. Leavitt - Direct

1 is featured prominently in the movie, and we worked with
2 them on that partnership.

3 Q. Okay. So in the movie, "Wreck-It Ralph" used the
4 eBay trademark —

5 A. Correct.

6 Q. — with your permission?

7 A. Correct.

8 Q. How does somebody get permission to use the eBay
9 trademark?

10 A. Basically, it goes through me. If someone is
11 requesting permission, my paralegal and myself will
12 prepare the licensing terms.

13 Q. Before you became the director of senior
14 intellectual property, what was your prior legal
15 experience?

16 A. So prior to that, I actually held the title of
17 director of global intellectual property for eBay, and
18 then prior — for about three years, two, three years —
19 and then, prior to that, I was the senior intellectual
20 property counsel for eBay.

21 Q. Okay. So in total, how many years have you worked
22 for eBay?

23 A. It will be nine years this June.

24 Q. Where is eBay located?

25 A. So eBay is headquartered in San Jose. I am actually

Ms. Leavitt - Direct

1 based in the Salt Lake City office.

2 Q. San Jose?

3 A. California.

4 Q. And they have an office in Salt Lake City.

5 A. Correct.

6 Q. Does eBay hold various trademarks, service marks,
7 trade names and service names that it has registered with
8 the United States Patent and Trademark Office?

9 A. Yes.

10 Q. Okay. If I refer to all of those as trademarks?

11 A. Correct. That's fine.

12 MR. McDONOUGH: May I approach the witness,
13 your Honor?

14 THE COURT: You may.

15 BY MR. McDONOUGH:

16 Q. Showing you what has been previously marked for
17 identification purposes is Government's Exhibit 1907.

18 Do you recognize Government's Exhibit
19 1907?

20 A. Yes.

21 Q. Have you seen those before?

22 A. Yes.

23 Q. What are those?

24 A. These appear to be certified copies of our trademark
25 registrations that are held with the United States Patent

Ms. Leavitt - Direct

1 and Trademark Office.

2 Q. Okay. And is Government's Exhibit 1907, which
3 consists of pages 1 through 64, is that a fair and
4 accurate certified copy of trademark registrations that
5 eBay has registered with the principal register of the
6 United States Patent and Trademark Office?

7 A. Yes.

8 Q. I would like to take a look at a couple of those
9 with you.

10 Ms. Chandler, could you please pull up
11 Government's Exhibit 1907, page 2. Do you recognize
12 this?

13 A. Yes.

14 Q. It is on the screen but — there will be a hard copy
15 in front of you.

16 What is this?

17 A. So this is a copy of our registration with the
18 United States Patent and Trademark Office for our eBay
19 logo.

20 Q. And how long — or when was this first put into use
21 by eBay?

22 A. So for the first use, it was in 2012 of the eBay
23 mark.

24 Q. Okay. And there are classes that these trademarks
25 are registered for?

Ms. Leavitt - Direct

1 A. Correct.

2 Q. What's the classes here that eBay has registered
3 this for?

4 A. You can see the classes are 35, 36, and 38.

5 Q. And what are those?

6 A. Different services. So the classes are divided
7 into two groups. So I believe it is class 1 through
8 34 is for actual hard goods, and 35 through beyond are
9 all four services. So these are all for different
10 services.

11 Q. And when was this trademark registered with the
12 United States Patent and Trademark Office?

13 A. This was registered in September of 2013.

14 Q. Okay. If we can go to page 5, and if you can please
15 zoom in on the top half, what is this?

16 A. This is a registration for the eBay word mark.

17 Q. All right. The first one had different
18 colors. This one is black and white. Is there a
19 difference?

20 A. Yes. The first was for the actual logo, and this is
21 for the plain text use of eBay.

22 Q. Okay. When was this first used by eBay?

23 A. So this was first used around 1995.

24 Q. When was it registered with the United States Patent
25 and Trademark Office?

Ms. Leavitt - Direct

1 A. So this was registered in January of 1999.

2 Q. Page 7, please. What is page 7?

3 A. So this is the registration for the buy-it-now
4 wordmark with the United States Patent and Trademark
5 Office.

6 Q. When was that first used?

7 A. This was first used in 1997.

8 Q. And when did eBay register this patent on the
9 United States Patent and Trademark Office principal
10 registry?

11 A. In September of 1999.

12 Q. Page 15, what is this?

13 A. So this is a copy of our registration for the
14 original eBay logo with the United States Patent and
15 Trademark Office.

16 Q. Okay. And first used?

17 A. So this one was first used in 1998.

18 Q. And registered?

19 A. This is registered in January of 2001.

20 Q. Okay. Has that logo changed over time?

21 A. Yes.

22 Q. And page 49, what is this?

23 A. So this is a registration for the buy-it-now
24 wordmark with the United States Patent and Trademark
25 Office.

Ms. Leavitt - Direct

1 Q. First used?

2 A. So this one was first used in 2000.

3 Q. And first registered?

4 A. This was registered in October of 2007.

5 Q. Okay. Have these trademarks been renewed over
6 time?

7 A. Yes.

8 Q. Over how long?

9 A. What do you mean by how long?

10 Q. How often do you have to renew a trademark?

11 A. So every ten years.

12 Q. Okay. All right. And have all these trademarks
13 been in use by eBay in that class since they have been
14 registered?

15 A. Yes.

16 Q. And now, I would like to show you a couple of
17 additional exhibits.

18 These have previously been identified, if we
19 could pull up Government's Exhibit 1431, page 80, please.
20 Thank you. All right.

21 This is a template page that was used to
22 induce individuals to provide information.

23 Do you see —

24 MR. O'SHEA: Objection to the form.

25 THE COURT: Sustained.

Ms. Leavitt - Direct

1 BY MR. McDONOUGH:

2 Q. Do you see any trademarks on page 8?

3 A. Yes.

4 Q. Can you please use the arrow, point out where the
5 trademarks are?

6 A. Yes. So that is the eBay logo mark.

7 Q. Okay. Does eBay use stars for its seller
8 ratings?

9 A. Yes.

10 Q. And if he could please zoom in on the fine print at
11 the bottom, please, Ms. Chandler.

12 Are there any trademarks in the fine
13 print?

14 A. Yes.

15 Q. Where would those be?

16 A. You can see the word "eBay" is used many times.

17 Q. What is the little — is there a little "c" there in
18 the bottom? What's the "c"?

19 A. That indicates it is a copyright.

20 Q. If we could zoom out and zoom in on the upper left
21 "eBay" word.

22 Do you see anything to the right of the word
23 "eBay" there?

24 A. The word "motors."

25 Q. Between "eBay" and "motors," do you see anything?

Ms. Leavitt - Direct

1 A. I see where you are saying. It looks like it is
2 probably a TM.

3 Q. What does a TM stand for?

4 A. It is used to designate a trademark.

5 Q. Okay. All right. If we could go to Government's
6 Exhibit 1432, page 15.

7 MR. McDONOUGH: Your Honor, may we have the
8 Elmo?

9 THE COURT: Certainly.

10 BY MR. McDONOUGH:

11 Q. Showing you what has been marked for identification
12 purposes as Government's Exhibit 1432, do you recognize
13 this.

14 A. Yes. I recognize, it looks like a page from eBay.

15 Q. Do you see any eBay trademark on Government's
16 Exhibit 1432?

17 A. Yes.

18 Q. Could you please point out where those are?

19 A. Yes. So this is the eBay logo.

20 Q. Is there anything to the right of the eBay
21 logo?

22 A. This appears to be — looks like a circle R
23 symbol.

24 Q. Okay. And what does the circle R symbol represent?

25 A. That's used to designate a registered trademark.

Ms. Leavitt - Direct

1 Q. Okay. Do you see any other trademarks on
2 Government's Exhibit 1432?

3 A. Yes.

4 Q. That's the buy-it-now trademark?

5 A. Correct.

6 Q. And then going to Government's Exhibit 1431, page
7 42, any eBay trademarks on this page?

8 A. Yes.

9 Q. Where would the eBay trademark be?

10 A. This is the registered eBay logo.

11 Q. Any other trademarks?

12 A. Yes. The eBay wordmark is used throughout the page
13 in different places.

14 Q. All right. And then, going to Government's Exhibit
15 1433, page 1, this is a screen shot.

16 Any eBay trademarks on this page?

17 A. Yes. The eBay wordmark is used in a couple of
18 different places.

19 Q. And could you point out where that might be?

20 A. It is right there, and then it is also used at the
21 bottom.

22 Q. Okay. With respect to those trademarks that you
23 identified, are those marks identical or
24 indistinguishable from the genuine trademarks as those
25 marks were in effect between the years 2007 and 2016?

Ms. Leavitt - Direct

1 A. Yes.

2 Q. Are you able to discern any differences between the
3 trademarks in those images and the genuine trademarks
4 registered by eBay as they were in effect between 2007
5 and 2016?

6 A. No.

7 Q. Did eBay give any person permission to use any of
8 those trademarks to trick users into providing personal
9 info or to infect users with a computer virus?

10 A. No.

11 Q. Does eBay protect its trademarks?

12 A. Yes.

13 Q. Why?

14 A. Trademarks are essential for identifying a company's
15 goods or services, and so consumers come to associate a
16 trademark with a company?

17 And if our trademarks are used on goods or
18 services that are below our standards or problematic in
19 any way, that serves to harm our reputation as a
20 business.

21 Q. How long has eBay been in business?

22 A. Since 1995.

23 Q. How many markets does eBay cover in the
24 United States or the world?

25 A. I believe currently we are in about 190 markets

Ms. Leavitt - Direct

1 worldwide.

2 Q. How did you find out about this case?

3 A. I was contacted by the United States Attorney's
4 Office.

5 Q. Okay. Have you ever heard of the words "Bayrob
6 Group"?

7 A. Yes.

8 Q. How have you heard of that?

9 A. In association with this case.

10 Q. Okay. Does your department, trademark department,
11 do any — did do any investigation regarding the Bayrob
12 Group?

13 A. This type of criminal matter would be handled by a
14 different group within legal.

15 Q. And when you say "within legal," what's legal?

16 A. So we have a department within the company that is
17 made up of attorneys and paralegals and different legal
18 specialists who support different legal needs that the
19 company may have.

20 Q. Did you do any work with the FBI in this
21 case?

22 A. No.

23 Q. Do you know, did your legal department do any work
24 with the FBI?

25 A. Yes.

Ms. Leavitt - Cross

1 MR. McDONOUGH: Thank you, no further
2 questions.

3 THE COURT: Mr. Goldberg.

4 CROSS EXAMINATION

5 BY MR. GOLDBERG:

6 Q. Couple questions. Good morning.

7 A. Good morning.

8 Q. As trademark counsel, would your job include
9 initiating actions to recoup damages suffered by the
10 company as a result of trademark infringement?

11 A. Depending on the context, yes.

12 Q. And is it safe for me to assume that you took no
13 such action regarding any trademark infringements related
14 to the Bayrob Group in your office?

15 A. Not myself personally. It was handled by a
16 different group within legal.

17 Q. Okay. And that was in a civil case or some kind of
18 claim for money damages?

19 A. I don't know that there is a claim for money
20 damages, but I know there is a different group in legal
21 that worked with the FBI on this case.

22 Q. Right. So the main context in which eBay defended
23 its trademark in this matter was through criminal action
24 with the FBI?

25 A. That's correct.

Ms. Leavitt - Cross

1 Q. And eBay sales last year were somewhere in the
2 neighborhood of \$10 billion dollars?

3 A. Probably more than that but —

4 Q. What do you think it was? Do you know?

5 A. I would say tens of billions of dollars.

6 Q. And you can't point to any particular money loss
7 associated with anything that the Bayrob Group, the
8 Defendants in this case or any other group associated
9 with Bayrob, may have taken?

10 A. It is hard to attach a specific monetary to
11 reputational damage that is caused by infringers.

12 Q. Right. So the answer would be is, you can't —

13 A. No.

14 Q. — say any money damages?

15 A. Not in this context, not a specific amount.

16 Q. With regard to security — and I know this is not
17 your department, so if you don't know, that's fine —
18 with regard to security in the eBay system, is there an
19 automated program or automated framework that goes
20 through the listings to try to detect any type of fraud
21 or misrepresentation prior to the potential customer
22 seeing the material?

23 A. We have a number of different systems in place to
24 identify different types of potential issues with
25 listings or with sellers.

Ms. Leavitt - Cross Cont'd

1 Q. And are they automated, or are they actually checks
2 that are performed by people?

3 A. It is a combination.

4 Q. And that is completely separate from your
5 department, and if there is a trademark issue, that comes
6 to you?

7 A. So my focus would be specifically on the systems
8 that are used to detect intellectual property
9 infringement, but there are other teams that have
10 different agreements.

11 Q. Okay. And intellectual property infringement, not
12 just on eBay's marks but on marks — the intellectual
13 property of items of manufacturers of items that are
14 being sold on eBay?

15 A. Correct.

16 MR. GOLDBERG: Thank you. I have nothing
17 further.

18 THE COURT: Cross, Mr. O'Shea?

19 MR. O'SHEA: Thank you.

20 CROSS EXAMINATION CONTINUED

21 BY MR. O'SHEA:

22 Q. Good morning, Ma'am. Can you see me over
23 here?

24 A. Yes, I can see you.

25 Q. Can we show the witness Exhibit 1431 that she just

Ms. Leavitt - Cross Cont'd

1 saw, the page 80 part?

2 MR. O'SHEA: Do we have to do that on Elmo?

3 THE COURT: She just brought it up.

4 MR. O'SHEA: Thank you.

5 BY MR. O'SHEA:

6 Q. All right. Do you remember seeing this document
7 just a short while ago, Ma'am?

8 A. Yes.

9 Q. I think there was some discussion about this mark at
10 the top, eBay. Do you see that, Ma'am?

11 A. Yes.

12 Q. Okay. And right next to it — I am going to put
13 that thing on there if I can — do you see that
14 little — what was — see where that arrow is, do you see
15 that?

16 A. Yes.

17 Q. Pretty small?

18 A. Yes.

19 Q. And you have to really squint and look at it. Am I
20 right about that?

21 A. Yes.

22 Q. Okay. You don't expect the average person looking
23 at an internet screen to notice that mark, do you?

24 MR. McDONOUGH: Objection.

25 THE COURT: Sustained.

Ms. Leavitt - Cross Cont'd

1 MR. O'SHEA: Okay. All right.

2 BY MR. O'SHEA:

3 Q. Now, looking at the bottom, Ma'am, do you see
4 all that? Do you remember being asked questions about
5 that?

6 A. Yes.

7 Q. Okay. That is what we call fine print, smaller
8 print than everything else. Do you agree with me about
9 that, Ma'am?

10 A. It is smaller than the print on the rest of the
11 page, correct.

12 Q. Smallest print on the page, fair enough?

13 A. Yes.

14 Q. Ms. Leavitt — am I pronouncing that correctly?

15 A. Yes, you are.

16 Q. Ms. Leavitt, to the best of your understanding of
17 all the eBay exhibits you were shown while on direct
18 examination, do you see any alterations to any of those
19 marks?

20 A. Not that I can tell based on the copy.

21 Q. Okay. And before you testified here this morning,
22 were you shown all these exhibits so you could be better
23 prepared to testify in front of the jury?

24 A. Yes.

25 Q. And who showed you those?

Ms. Leavitt - Cross Cont'd

1 A. The prosecutor who was just questioning me.

2 Q. Okay. How long did that meeting take?

3 A. Less than an hour.

4 Q. Okay. And during that meeting, you were like I am
5 doing here with this arrow here, you were shown, "be on
6 the lookout for this business and that trademark," all
7 that, the meeting was about that, right?

8 A. It was more just making sure I could see the
9 trademarks on the different pages.

10 Q. Okay. So you knew exactly what to point to so we
11 wouldn't waste time on the stand. Fair enough?

12 A. Yes.

13 Q. Now, do you know what a cookie is?

14 A. Yes.

15 Q. Does eBay plant cookies on people's web pages when
16 they visit eBay so the can better direct them to their
17 purchasing habits?

18 A. I am not familiar with whether we do or not.

19 Q. Okay. Do you know why when you go to an eBay page
20 that certain products that you purchased in the past
21 might automatically pop up?

22 A. No. It is not my area of responsibility.

23 Q. Okay. Do you know — do you know as part of your
24 job responsibilities who secures your web pages, what
25 company?

1 A. No. It — well, it depends on the context.

2 Q. Has it been Norton and Symantec in the past,
3 Ma'am?

4 A. Symantec, yes, I am familiar with Symantec. Norton
5 I am not a hundred percent on.

6 MR. O'SHEA: Okay. Thank you. No further
7 questions.

8 THE COURT: Redirect?

9 MR. McDONOUGH: No, your Honor.

10 THE COURT: Step down. Call your next
11 witness.

12 MR. LEVINE: Your Honor, we have a
13 stipulation we would like to put on the record.

14 THE COURT: All right.

15 MR. LEVINE: So the parties, the
16 United States and the Defendants stipulate that the
17 trademark witnesses from two other companies, Western
18 Union and Symantec, need not testify in this matter; that
19 witnesses from Western Union and Symantec would testify
20 that the trademark certifications marked as Government's
21 Exhibits 1901 and 1903 are fair and accurate compilations
22 of trademarks registered on the principal register of the
23 United States Patent and Trademark Office.

24 Witnesses from Western Union and Symantec
25 would further testify that Western Union and Symantec

1 marks appear on Government's Exhibits 1248, 1421, 2105,
2 2107, and 2108.

3 The marks on these exhibits are identical or
4 indistinguishable from the genuine registered marks by
5 Western Union and Symantec.

6 Further, these witnesses would testify that
7 neither Western Union nor Symantec gave the Defendants
8 permission to use any of their marks for purposes of
9 either tricking users into clicking on attachments and
10 getting malware or tricking users into becoming money
11 mules.

12 And finally, these witnesses would testify
13 that Western Union and Symantec are harmed when others
14 use their marks in this manner without permission of the
15 true owner of the mark.

16 THE COURT: Mr. O'Shea?

17 MR. O'SHEA: So stipulated.

18 THE COURT: I'm sorry. I'm sorry.

19 Mr. Goldberg first.

20 MR. GOLDBERG: So stipulated.

21 THE COURT: Mr. O'Shea?

22 MR. O'SHEA: So stipulated Judge.

23 THE COURT: And again, to remind you,
24 stipulations are facts agreed to by and between the
25 parties.

Mr. Frost - Direct

1 MR. LEVINE: The United States would now
2 like to call Matthew Frost, your Honor.

3 THE COURT: Mr. Frost, please step up to the
4 podium.

5 MATTHEW FROST

6 called as a witness by and on behalf of the Government,
7 being first duly sworn, was examined and testified
8 as follows:

9 THE COURT: Please take a seat over there.

10 DIRECT EXAMINATION

11 BY MR. LEVINE:

12 Q. Good morning.

13 A. Good morning.

14 Q. You have a little mike in front of you. You can
15 move that mike a little closer to you. And you can pull
16 it up a little bit so you can speak right into it, and
17 your chair moves a little bit. We want to make sure
18 everybody can hear you.

19 If you would please state and spell your
20 last name for the court reporter?

21 A. Matthew Frost, M-a-t-t-h-e-w, F-r-o-s-t.

22 Q. Mr. Frost, what do you do?

23 A. I am a computer forensic examiner for the Federal
24 Bureau of Investigation.

25 Q. Okay. And Forensic Examiner Frost were you

Mr. Frost - Direct

1 physically present in Romania during the search of Bogdan
2 Nicolescu residence?

3 A. Yes.

4 Q. And did you also make image copies of some of the
5 digital devices, the computers and hard drives found in
6 Bogdan Nicolescu's residence?

7 A. Yes.

8 Q. First, I want to go through your background. What
9 is your educational background?

10 A. I have both a Bachelors and a Master's Degree from
11 Idaho State University. I have a Bachelor's Degree in
12 Economics and a Master's of Business Administration with
13 an emphasis in information assurance.

14 Q. Okay. What is an MBA with a Master's in information
15 assurance. What is information assurance?

16 A. Information assurance was additional classes I had
17 to take to get the emphasis with my masters, and
18 information assurance is the securing of data for large
19 corporations or businesses. It is keeping the data safe
20 and secure.

21 Q. Okay. And prior to working with the FBI, did you
22 spend a couple of years in Eastern Europe?

23 A. Yes, I did.

24 Q. Can you tell us about that?

25 A. Yes. I lived in the Ukraine, and I was there for

Mr. Frost - Direct

1 two years from 2001 until 2003 on a church service
2 mission that was self-funded.

3 Q. Okay. And you said you worked for the FBI. When
4 did you begin working for the FBI?

5 A. My employment began in 2007.

6 Q. Okay. So that's about 12 years ago?

7 A. Yes.

8 Q. All right. And where is your office with the
9 FBI?

10 A. I am located in Pocatello, Idaho.

11 Q. And is that where you came from to testify
12 today?

13 A. Yes.

14 Q. You said you were a forensic examiner. What is a
15 forensic examiner?

16 A. Forensic examiner is a computer tech position within
17 the FBI where we take devices that have been seized or
18 are given over for consent search with legal authority,
19 and I take those devices.

20 I make perfect copies of the data and then
21 extract data from these devices, whether it is a
22 cellphone, a computer, a GPS, whatever the data, extract
23 the data, and I make it available for agents to review or
24 turn it over to the Court or Court proceedings.

25 Q. So you copy the data and make it available for

Mr. Frost - Direct

1 others to review?

2 A. Yes.

3 Q. And as a forensic examiner for the FBI roughly how
4 many computers and hard drives would you say you have
5 examined?

6 A. Over my career it is thousands, over 6,000 devices.

7 Q. Over 6,000 did you say?

8 A. Yes.

9 Q. And how many searches of businesses or residences
10 have you assisted with roughly?

11 A. Dozens.

12 Q. Do you have any certifications?

13 A. Certifications?

14 Q. Yes.

15 A. So I am certified forensic examiner by the
16 FBI.

17 Q. And do you have any other certifications?

18 A. I have taken vendor training so training by an
19 outside entity from the FBI where you take a class, and
20 at the end of the class, there is a test and a
21 certification that comes with that test.

22 Q. And is that a certification to use their particular
23 product?

24 A. In some cases, their product or it is a knowledge
25 and a topic related to computer forensics.

Mr. Frost - Direct

1 Q. Okay. And have you attended trainings on visual
2 forensics?

3 A. Yes.

4 Q. Since you joined the FBI in 2007, approximately how
5 many trainings have you attended per year?

6 A. It is probably about two per year, some years three
7 or four; some years one.

8 Q. All right. And how long was each of those
9 trainings?

10 A. Each of them is usually a week of 8-hour days.

11 Q. And do you train other FBI employees?

12 A. Yes. I am an instructor for the FBI on digital
13 forensics.

14 Q. And what portions do you teach?

15 A. Courses on cellphones, on introduction to forensics
16 or the beginner forensic courses and cyber courses.

17 Q. And have you testified as an expert in federal court
18 before?

19 A. Yes, I did.

20 Q. And what was the general subject matter of that
21 case?

22 A. The case was a child prostitution case.

23 Q. Okay. And did the Court qualify you as an expert in
24 that case?

25 A. Yes, they did.

Mr. Frost - Direct

1 Q. That was yes?

2 A. Yes.

3 Q. Had you received any awards through your work with
4 the FBI?

5 A. Yes. I received an award from the office of the
6 Director of National Intelligence.

7 Q. And what was that award for?

8 A. It was for work I did on the Alpha Bay case.

9 Q. What is or was Alpha Bay?

10 A. Alpha Bay is a dark web marketplace and dark web —
11 it is part of the worldwide web, and to get to it, you
12 have to use special software. I kind of think of it
13 as a library. So if the internet is the library
14 or the worldwide web, any websites you can freely go
15 to?

16 The dark web is a portion of that library
17 that you can only get to it if you know how to get there.
18 It is not restricted by any means, but to get there, you
19 have to know how to use the specialized software to
20 access that portion of the library or the dark web.

21 Q. Okay. And so this was a website on the dark
22 web?

23 A. Correct.

24 Q. And what was Alpha Bay doing on the dark web?

25 MR. GOLDBERG: Objection.

Mr. Frost - Direct

1 THE COURT: Overruled. You may answer, sir.

2 THE WITNESS: Thank you.

3 A. Alpha Bay was a marketplace or an online store
4 front, if you will, where users could go and either buy
5 or sell various products, most of them illegal, drugs,
6 prostitution services.

7 You could hire a hit man, other illegal
8 things where you could pay and/or sell, you could buy or
9 sell items that you can't find readily available, and you
10 can pay in a way that tries to keep your identity
11 anonymous.

12 Q. Could you buy stolen credit cards?

13 A. Yes, you could.

14 Q. And could you buy and sell stolen identities?

15 A. Yes.

16 Q. And when did you get this award related to your work
17 with Alpha Bay?

18 A. I don't remember exactly. The search was in 2017.
19 It was during 2018 sometime. I didn't go to the awards
20 ceremony. I just got notification and then the
21 certificate in the mail.

22 Q. All right. I want to take you now on your trip to
23 Romania.

24 Did you you travel to Romania in September
25 2016 to assist with the searches and arrests in the

Mr. Frost - Direct

1 Bayrob investigation?

2 A. Yes.

3 Q. Now, prior to traveling to Romania in September
4 2016, had you had any involvement in the Bayrob
5 investigation?

6 A. No.

7 Q. How did you get — end up getting roped into going
8 to Romania in 2016 to assist with the searches and
9 arrests in the Bayrob investigation?

10 A. A request came in from our headquarters office.
11 They asked for people with knowledge on Linux operating
12 systems to assist in a large search.

13 Q. What is Linux?

14 A. Linux is an operating system, much like the windows
15 operating system is the operating system, that runs the
16 basic functions of a computer.

17 But Linux is a free and open source software
18 or an operating system that anyone can download use and
19 install on their computers for free.

20 Q. Okay. And did you have Linux experience?

21 A. Yes.

22 Q. And is Linux experience rare within the FBI?

23 A. It is, yes. Most of the examinations we get are
24 windows or Mac or cellphone related, so to be
25 specialized and have the knowledge for Linux it is

Mr. Frost - Direct

1 limited within the FBI.

2 Q. When you got to Romania, were you assigned to a
3 particular search location?

4 A. Yes, I was.

5 Q. Which location were you assigned to?

6 A. It was a residence in Brasov, Romania.

7 Q. Do you know whose residence that was?

8 A. It was —

9 Q. Was it Bogdan Nicolescu?

10 A. It was Bogdan Nicolescu, excuse me.

11 Q. And when did you travel to Braosov, Romania?

12 A. We traveled up to Brasov on the 27th of September.

13 Q. And that's 2016?

14 A. 2016.

15 Q. And who did you travel to Brasov with?

16 A. With Special Agent Ryan MacFarlane and Peter Traven
17 from the FBI that was working out of the U.S. Embassy in
18 Romania.

19 Q. Okay. Peter Traven was working out of the U.S.
20 Embassy in Romania?

21 A. Yes.

22 Q. Were you involved in the search of Bogdan
23 Nicolescu's residence on September 28, 2016?

24 A. Yes.

25 Q. And how did you get to Bogdan Nicolescu's residence

Mr. Frost - Direct

1 on September 28, 2016?

2 A. I traveled with Pete Traven in his embassy vehicle.

3 Q. And approximately what time did you arrive at Bogdan
4 Nicolescu's residence on September 28?

5 A. It was early morning. I don't remember exact time.
6 It was between 5:00 a.m. and 6 a.m. I know the hotel
7 breakfast wasn't available so it was early.

8 Q. Why did you arrive so early in the morning?

9 A. We arrived early in the morning, we — the FBI had a
10 cooperating source that was trying to keep members of the
11 group online.

12 MR. O'SHEA: Objection.

13 THE COURT: Sustained.

14 BY MR. LEVINE:

15 Q. Generally, why 5:00 or 6:00 in the morning?

16 A. We wanted to get there early in the morning so that
17 we could hopefully — we wanted to get a computer in an
18 unlocked state.

19 Q. And did you have information to suggest that it was
20 more likely — that that was more likely to happen early
21 in the morning?

22 A. Yes.

23 Q. Now, how would you describe the area where
24 Bogdan Nicolescu's residence was located on September 28,
25 2016?

Mr. Frost - Direct

1 A. The residence was outside of City Center. It was a
2 personal residence or a home, an apartment building
3 towards the end of a street. I remember it being dark,
4 early in the morning. There were no lights on.

5 Q. Okay. I'm sorry. Did you say it was a home or an
6 apartment building?

7 A. It was a home, a personal dwelling.

8 Q. And how would you describe the perimeter of Bogdan
9 Nicolescu's residence?

10 A. The perimeter had a large concrete or cinder block
11 fence around with a large cast iron metal gate that led
12 to the driveway.

13 Q. How tall would you say that wall was around the
14 residence?

15 A. It was probably 6 or 8 feet tall. It was taller
16 than I was.

17 Q. And when you arrived at the house, were you able to
18 see anything inside the house?

19 A. We couldn't see anything inside the residence.

20 Q. Who attempted to enter the house first?

21 A. The Romanian National Police had a team of folks
22 similar to like a SWAT team or a special tactics team
23 that entered the residence first.

24 Q. Okay. And roughly how many RNP attempted to enter
25 the house?

Mr. Frost - Direct

1 A. I believe there were six on their team.

2 Q. And how did they attempt to enter the house
3 initially?

4 A. They went up to the — they were grouped into little
5 teams of two or three, and some were in the front, and
6 some in the back. The first team or the breaching team
7 announced who they were and then hit the door with a
8 battering ram.

9 Q. What is a battering ram?

10 A. It was a large metal device that is used to
11 knock open a door if we don't have a key or if it is not
12 open.

13 Q. And were the RNP able to break down the front door
14 with a battering ram?

15 A. No. The front door appeared to be reinforced. They
16 hit it several times. It took so long that I remember,
17 as we were sitting out in the cars waiting for the team
18 to enter the building, someone came to the window on the
19 second floor between the first and second floor and
20 started yelling down to them in Romanian.

21 Q. Was that from the Nicolescu residence or someone in
22 another house?

23 A. That was from the Nicolescu residence they were
24 trying to enter.

25 Q. Okay. Were the RNP ever able to get into the

Mr. Frost - Direct

1 house?

2 A. Yes. After the failed attempt on the front door,
3 they went around back and entered through the back.

4 Q. Did you see how they were able to enter in through
5 the back?

6 A. Yes. The back of the home had a — it is like a
7 French door that swung open, and they broke the latch
8 mechanism between the two doors, and they freely swung
9 open, and they entered.

10 Q. Okay. And at some point, did you enter the
11 house?

12 A. Yes. We —

13 Q. When did you enter the house?

14 A. I entered the home after the Romanian National
15 Police had gone through the entire residence and what was
16 usually termed as they cleared the house, as in they
17 verified there were no threats to the rest of the team,
18 to come into the building;

19 That everyone in the home was accounted for,
20 and all the areas posed no imminent threat to the rest of
21 the team coming in.

22 Q. Okay. And did you enter through the broken glass
23 door in the back?

24 A. Yes, we did.

25 Q. Once you entered, who was in the house?

Mr. Frost - Direct

1 A. When I entered, the Romanian National Police were in
2 the house, and the — the person that was in the home
3 that had been yelling from the window was there with
4 them.

5 Q. And who was that person?

6 A. He was in handcuffs. That was Bogdan Nicolescu.

7 Q. He was in handcuffs at that point?

8 A. Yes, he was.

9 Q. And who else was in the home?

10 A. The Romanian National Police, myself, and Pete
11 Traven.

12 Q. And was anyone else in the home?

13 A. No one else was in the home.

14 Q. And you said Nicolescu was in handcuffs at the time
15 you entered?

16 A. Correct.

17 Q. Was he handcuffed the whole time, or did they come
18 off at some point?

19 A. We were at the residence for several hours that day,
20 and at the beginning of the search, as we went around
21 from room to room, he was in handcuffs.

22 Towards the end of the search, as we were
23 completing and gathering all the items that had been
24 seized, he was not in handcuffs, and he was free to move
25 about the home with the escort from the Romanian National

Mr. Frost - Direct

1 Police.

2 Q. And do you know when you got there, was Nicolescu
3 given an opportunity to contact a lawyer or a trusted
4 person?

5 A. Yes.

6 Q. Okay. And did any lawyer or trusted person show
7 up?

8 A. Yes. We waited — we didn't do any of the work. We
9 didn't touch the computer systems or go through any
10 items. We waited for — I can't remember the exact
11 amount of time we indicated waited. It was a little
12 while.

13 I remember I could have gone back to the
14 hotel and got breakfast, but I don't know how long it
15 was.

16 Q. So you waited, but you remember it was long enough
17 that you could have gone back and gotten breakfast during
18 that time?

19 A. Yes. I had a Granola bar that was in my bag.

20 Q. Okay. Were you involved in the search of the
21 house?

22 A. I assisted the Romanian National Police with the
23 search.

24 Q. So what did that assistance look like?

25 A. We were a guest in the country. The Romanians had

Mr. Frost - Direct

1 the legal authority to search the house, and I was there
2 as the technical expert for the FBI to verify their
3 procedures and that the evidence matched our procedures
4 so nothing was contaminated or tainted or not used
5 correctly.

6 Q. But what did you do? Physically what did you do
7 during the search?

8 A. So we went from room to room in the home and located
9 all computer equipment that could have stored information
10 or data that we could have searched later.

11 Q. So you went from room to room with the RNP?

12 A. Yes.

13 Q. And in general how would you describe the inside of
14 Nicolescu's house?

15 A. It was a larger residence, main floor. There was an
16 office type area on the main floor, kitchen in between
17 the first and second floor. Upstairs there were three
18 bedrooms, two bathrooms.

19 Q. Two bathrooms upstairs?

20 A. Yes.

21 Q. Okay. And you said there was a kitchen area
22 between the first and second floor. Can you explain
23 that?

24 A. Yeah. It was kind of an offset. So if you entered
25 the home, there was a living room, family room area, and

Mr. Frost - Direct

1 you went up a stairs part way, and there was a kitchen
2 and dining room area and went up the rest of the stairs
3 into the living quarters, bedrooms, bathrooms.

4 Q. And was there also a basement or garage level?

5 A. There was down the stairs, yes.

6 Q. And so who went around to each of these rooms?

7 A. The Romanian National Police, myself, and Bogdan
8 Nicolescu was escorted with the police in every room we
9 went to.

10 Q. And was Special Agent Ryan MacFarlane there as
11 well?

12 A. Yes, he was.

13 Q. And what would happen in each room?

14 A. In each room, we identified computer systems,
15 cellphones, the networking gear, and initially, we
16 located, determined if it was on or off. We looked to
17 see if they were in a state that they were unlocked or if
18 the screen was opened or if you had to type in a password
19 to access the computer system.

20 Q. And once they found the device that they potentially
21 wanted to seize, what would they do with it?

22 A. Once we located the device, we wrote the identifying
23 information off of it, serial numbers, make and models,
24 any identifiable marks, and then all of them were locked
25 or in an offstate. So we weren't able to access any of

Mr. Frost - Direct

1 the data on scene. So they were either shut down or
2 unplugged, or if they were already unplugged, they were
3 moved to a central location that they could be cataloged
4 for seizure.

5 Q. And did the RNP find hard drives and computers
6 throughout the house?

7 A. Yes.

8 Q. Could you tell if any of the computers around the
9 house were connected?

10 A. Yes. There was a network for — there was cables
11 going from an area in the kitchen, kind of the back of
12 the kitchen, where some of the computer equipment was
13 with a router?

14 And there were cables running outside the
15 kitchen around to the office area and up to other areas
16 of the home. So the computers were connected. Some of
17 them were connected in a wired fashion.

18 Q. So these were physical network cables?

19 A. Yes.

20 Q. And in your experience having done many of these
21 searches was that unusual?

22 A. It was —

23 MR. GOLDBERG: Objection.

24 THE COURT: Sustained.

25

Mr. Frost - Direct

1 BY MR. LEVINE:

2 Q. Have you ever seen computers networked like this in
3 the search of a home?

4 A. Not exactly like this, no.

5 Q. In 2016, the year you did the search, how would you
6 typically see computers in a house connected?

7 MR. GOLDBERG: Objection.

8 THE COURT: Overruled. You may answer.

9 A. Usually, in a residence, there is a central location
10 where the router will sit, and there may be one computer
11 connected physically, and there is a wireless network
12 where all the other devices connect wirelessly.

13 Q. In your training and experience, is there any reason
14 to use network cables running around the house instead of
15 wireless as you just described?

16 MR. GOLDBERG: Objection.

17 THE COURT: Overruled.

18 A. Wireless is less secure as in everyone that is in
19 the radius of the broadcast can see the broadcast, and
20 depending on if the wireless is encrypted, they are more
21 secured. They might be able to access the network and
22 connect that way. Usually, hardline connections are
23 quicker as in there is other traffic and transport pass
24 over wires than wireless.

25 Q. Okay. So quicker and more secure?

Mr. Frost - Direct

1 A. Yes.

2 Q. All right. So did you have a chance to review the
3 digital devices on this hand dolly that is in front of
4 you last night?

5 A. Yes, I did.

6 Q. And does this dolly or hand truck contain some of
7 the digital devices found in Bogdan Nicolescu's residence
8 on September 28, 2016?

9 A. Yes.

10 Q. I want to go through some of these with you.

11 First, I am bringing the witness what has
12 previously been marked as Government's Exhibit 1. What
13 is Government's Exhibit 1?

14 A. It is an Asus cellphone.

15 Q. Okay. And where was it recovered?

16 A. This was located upstairs in the bedroom.

17 Q. The bedroom in Bogdan Nicolescu's residence?

18 A. Yes.

19 Q. And how do you know this is that cellphone?

20 A. When I was in Romania, I took the back off, and
21 there is identifying information on the back of the phone
22 that is like a serial number.

23 Q. And to save time, did you review all the serial
24 numbers on the different devices we have here and compare
25 them to your notes to confirm they are the same serial

Mr. Frost - Direct

1 numbers?

2 A. Yes. These items match the serial numbers that I
3 recorded when I was on scene in Romania.

4 Q. I am showing you now Government's Exhibit 65, and
5 can you tell us what is Government's Exhibit 65?

6 A. This is a Samsung cellphone.

7 Q. And where was Government's Exhibit 65 recovered?

8 A. It was also upstairs in the residence in the
9 bedroom.

10 Q. Okay. And that was the residence being Bogdan
11 Nicolescu's residence?

12 A. Yes.

13 Q. And I am showing you what has previously been marked
14 as Government's Exhibit 2041. Do you recognize
15 Government's Exhibit 2041?

16 A. Yes. It is an Acer laptop.

17 Q. And where was the Acer laptop recovered?

18 A. This was also upstairs in the residence in the
19 bedroom.

20 MR. GOLDBERG: What was the number on that?

21 MR. LEVINE: 2041.

22 MR. GOLDBERG: Thank you.

23 BY MR. LEVINE:

24 Q. And showing you what has previously been marked as
25 Government's Exhibit 2042, what is Government's Exhibit

Mr. Frost - Direct

1 2042?

2 A. This is a think pad laptop from de novo.

3 Q. And where was Government's Exhibit 2042 recovered?

4 A. This was also in the residence, in the bedroom
5 upstairs.

6 Q. Okay. And I am showing you a hard drive that has
7 previously been marked as Government's Exhibit 2003.

8 Do you recognize Government's Exhibit
9 2003?

10 A. Yes. That's a Samsung hard drive.

11 Q. Okay. And where was that Samsung hard drive located
12 or recovered?

13 A. This was located in the office of the residence
14 downstairs on the main floor.

15 Q. Was it in a computer or just sitting in the
16 office?

17 A. It was just a bare hard drive sitting out.

18 Q. Okay. And let me show you — I am showing you now
19 what has just been marked as Government's Exhibit 2046.
20 What is Government's Exhibit 2046?

21 A. This is a ZTE router.

22 Q. And where was that located?

23 A. This was in the kitchen.

24 Q. The kitchen of the Nicolescu residence?

25 A. Yes.

Mr. Frost - Direct

1 Q. And then — now, we are going to test the limits of
2 my strength.

3 With the great assistance of Assistant
4 United States Attorney McDonough, I am showing you
5 what has previously been marked as Government's Exhibit
6 2040. Do you recognize that it is an HP desktop
7 computer?

8 A. Yes.

9 Q. And where was that located?

10 A. This was located in the kitchen in close proximity
11 to the router kind of in the back of the kitchen.

12 Q. Okay. So I am not going to lift this.

13 I am pointing to a tower, computer tower
14 marked as Government's Exhibit 2038?

15 THE COURT: Did you say 2038?

16 MR. LEVINE: 2038.

17 BY MR. LEVINE:

18 Q. What is Government's Exhibit 2038?

19 A. 2038 is a large black computer or server is what I
20 would term it.

21 Q. What is a server? How is that different from a
22 computer?

23 A. Server differs from a personal computer. Usually,
24 based on size, you can tell the power, processing
25 capacity. It is able to handle more connections, more

Mr. Frost - Direct

1 computations. It has got a bigger power supply to handle
2 more stuff going on inside the system and, hence,
3 cooling, so it doesn't overheat.

4 Q. So it is an enhanced computer?

5 A. Yes.

6 Q. And where was that located?

7 A. This was located upstairs in the residence in one of
8 the bedrooms.

9 Q. And how many hard drives were in this computer or
10 server?

11 A. Five.

12 Q. Five. Is that standard for a personal computer to
13 have five hard drives?

14 MR. GOLDBERG: Objection.

15 THE COURT: Overruled.

16 THE WITNESS: No. That is not standard.

17 BY MR. LEVINE:

18 Q. How many hard drives does a personal computer
19 usually have?

20 A. Personal computer usually has a single hard drive
21 when it comes from the factory, sometimes two.

22 Q. And what was the sizes of the hard drives in this
23 computer?

24 A. I don't remember the exact range. They range from
25 500 gigabytes to a terabyte or two terabyte.

Mr. Frost - Direct

1 Q. What is a terabyte?

2 A. A terabyte is a thousand gigabytes. A gigabyte is a
3 thousand megabytes. So if we talk about size in
4 something, we know like a music CD holds 700 megabytes of
5 data. So a terabyte would be many, many times that,
6 where you could store hundreds, if not thousands, of CDs
7 on a single terabyte.

8 Q. If we were to compare in terms of paper in terms of
9 trees, do you remember how many trees that would be?

10 A. They approximated it would be about 50,000 trees cut
11 down turned into paper if you were going to take a
12 terabyte in documents and print them all out.

13 Q. So we won't print them today.

14 Were any of these five drives encrypted?

15 A. Yes.

16 Q. How many of the five drives in here were encrypted?

17 A. All five were encrypted.

18 Q. And what type of encryption was used?

19 A. LUKS encryption.

20 Q. What is LUKS encryption?

21 A. LUKS encryption is the type of encryption that is
22 used on Linux systems and the encryption is like the lock
23 on the room in a house. They look at a hard drive as a
24 home, it is partitioned or broken down into segments like
25 rooms in a house, and each room in the house can have a

Mr. Frost - Direct

1 door that is either open or close and can have a lock.

2 So you can't unlock it unless you have the password or a
3 way to get into that room.

4 Q. Did the FBI try to unlock these rooms to use your
5 metaphor?

6 A. Yes.

7 Q. And was the FBI able to decrypt any of the hard
8 drives on this computer?

9 A. No.

10 Q. When the computer was seized, was it in this shape,
11 kind of dented a little bit?

12 A. It was not.

13 Q. How did that happen?

14 A. We — when we seized it and it was in Romania, it
15 was in pristine — well, it was in a lot better
16 condition, not broke or bashed in. During shipment, it
17 was likely dropped. Something caused the damage to
18 happen. However, the drives inside the computer were all
19 still — we were able to read those drives, and they were
20 accessible.

21 Q. When you say you could read them and accessible were
22 they still encrypted?

23 A. Yes. I could look and see the rooms and see they
24 were encrypted, but I couldn't get to the data inside
25 those encrypted partitions.

Mr. Frost - Direct

1 Q. Is it possible that any of the damage caused to this
2 computer in transit caused any of those hard drives to
3 become encrypted?

4 A. No.

5 Q. Okay. We are going to take this one down. I am
6 going to ask the witness to come down to look at this
7 one. Okay. Computer Forensic Examiner Frost, what is —
8 what is the Government's Exhibit number?

9 A. 2039.

10 Q. And what is Government's Exhibit 2039?

11 A. 2039 is — it is a Dell Power Edge server.

12 Q. Okay. And was this found in Bogdan Nicolesu's home
13 as well?

14 A. Yes.

15 Q. Where was this found in Bogdan Nicolescu's home?

16 A. This was located in what we termed the office on the
17 main floor.

18 Q. And how many drives, hard drives are there inside
19 this computer?

20 A. There were eight hard drives inside this computer.

21 Q. Eight hard drives.

22 And what was the size of the hard drives in
23 this computer?

24 A. This computer had two terabyte hard drives, a total
25 of 16 terabytes of storage.

Mr. Frost - Direct

1 Q. So 16 terabytes of hard drives in this computer in
2 total?

3 A. Yes.

4 Q. And was there anything unusual about how this
5 computer was set up?

6 A. The setup was a server designed to accommodate large
7 amounts of storage like — the only time I have seen a
8 setup similar to this is when I entered a data center or
9 a business.

10 Q. And what is a data center?

11 A. Data center is where companies host their content
12 that has power and cooling, and they stack lots and lots
13 of servers in a manner that can be connected to the
14 internet so the data can be accessed.

15 Q. Okay. When this computer was seized, was it all put
16 together like this?

17 A. It was not. The case was open and the hard drives,
18 the ones that are on the inside, four of them, were
19 hanging out, and the ones in the front here were inside
20 of it.

21 Q. Okay. So did it appear as though it was just being
22 put together?

23 A. Yes. It looked like it was being worked on or maybe
24 assembled.

25 Q. And have you ever seen a computer like this one in a

Mr. Frost - Direct

1 residence?

2 MR. GOLDBERG: Objection.

3 THE COURT: May I see you at side bar?

4 (Side bar held on the record.)

5 THE COURT: I agree he is an expert, but I
6 know you've objected to a couple questions similar to
7 this one.

8 MR. GOLDBERG: Right.

9 THE COURT: And I am assuming the basis is,
10 it is really not part of his expertise.

11 MR. GOLDBERG: Correct. And I could be
12 wrong — and I know I will be corrected — but I never
13 received an expert report saying that this opinion that
14 these machines are not found in residences on a regular
15 basis.

16 MR. LEVINE: He was notified as an expert.
17 His resume was provided. It said — I believe my
18 recollection that it said he would testify about the
19 devices he identified in the residence.

20 THE COURT: The problem I am having — and I
21 have given you great latitude up to now — I agree he is
22 an expert. But I still think you need a little more
23 foundation for some of these questions, particularly in
24 this area. And that's why I, again, I have given great
25 latitude, but now it is like —

Mr. Frost - Direct

1 MR. LEVINE: I will lay more foundation.

2 MR. GOLDBERG: Your Honor, do you think we
3 can take a break?

4 THE COURT: We are off the record.

5 (Discussion held off the record.)

6 (Side bar concluded.)

7 BY MR. LEVINE:

8 Q. Forensic Examiner Frost, can you demonstrate how the
9 hard drives are put into this computer?

10 A. Certainly. On the front four of the hard drives are
11 located in the bays on the front of the server that can
12 easily be pulled out and switched out.

13 Systems like this are designed, so if a
14 drive goes bad, you can pull it out, replace the drive,
15 stick it back in, and then the data rebuilds itself
16 because of the way the system is set up.

17 All the data is put across all the drives
18 and not just one hard drive or a single point of failure.
19 So like I say, in a data center or businesses where loss
20 of data is critical, four of them go here, and the other
21 ones are connected with power and data connected right
22 here. So that's how they all go.

23 BY MR. LEVINE:

24 Q. So is this computer also expandable in that you
25 could add more, bigger hard drives or more hard

Mr. Frost - Direct

1 drives?

2 A. Yes. Yes, it is.

3 Q. Okay. And if he — I know this is heavy, but if we
4 could just turn it around so we can see this side, can
5 you explain what we are seeing up at the top of the back
6 of this exhibit?

7 A. Certainly. These are two power supplies for the
8 server. So it has two power supplies. In case one of
9 the power supplies goes bad or stops working, it won't
10 kill the server as redundant power supplies coming from
11 two sources.

12 So again, in the event of a failure on one
13 of them, it would still be able to work while you replace
14 the power supply to restore it to its full operating
15 order.

16 Q. And is that a standard feature of a standard
17 computer?

18 A. No.

19 MR. GOLDBERG: Objection.

20 MR. O'SHEA: Objection.

21 THE COURT: Sustained.

22 BY MR. LEVINE:

23 Q. In your experience where have you seen a dual power
24 supply like this?

25 MR. GOLDBERG: Objection.

Mr. Frost - Direct

1 THE COURT: Overruled.

2 A. Dual power supplies are located on computers or
3 servers where, if one drive goes bad, you will lose data.
4 So on computers or servers, oftentimes in data centers
5 where you need two power supplies so that — I'm sorry.

6 They are loaded on computers that are —
7 they want the user, the owner wants them to be on all the
8 time, so if one of them goes bad, it doesn't kill their
9 server.

10 Q. So where failure is not an option.

11 A. Correct.

12 MR. LEVINE: Okay. Your Honor, now would be
13 a good time to take a break.

14 THE COURT: Ladies and gentlemen, we
15 will take our morning recess. Please remember the
16 admonition.

17 (Recess had.)

18 THE COURT: Please be seated. You may
19 continue, Mr. Levine.

20 BY MR. LEVINE:

21 Q. Forensic Examiner Frost, I am going to hand you a
22 hard copy of Government's Exhibit 5 and bring that up and
23 then show the ladies and gentlemen of the jury,
24 Mr. Frost, what is Government's Exhibit 5?

25 A. I am sorry. Can I move this microphone? The cable

Mr. Frost - Direct

1 is like bound on this side, and it is like I am stuck in
2 the corner.

3 THE COURT: Sure go right ahead.

4 (Pause.)

5 Q. All right. If you just speak into the microphone,
6 hopefully we will be able to hear.

7 So I showed you Government's Exhibit 5. Can
8 you tell us what Government's Exhibit is?

9 A. Yes. It is a document that we sign when we were in
10 the residence as we were going through the process of
11 gathering all the items, and before we left, we signed
12 each page of this document.

13 Q. All right. And is it an inventory form?

14 A. A lot of it is in Romanian but —

15 Q. You will see halfway through is the translation
16 copy?

17 A. Yes. A lot of it is serial numbers and items that
18 we located in the residence, and they were entered in by
19 the Romanian National Police before we left, and yes, it
20 looks like it has an inventory of all the items that were
21 seized.

22 Q. Were you physically present when the Romanian
23 National Police inventoried the devices they were going
24 to seize from Mr. Nicolescu's home?

25 A. Yes.

Mr. Frost - Direct

1 Q. And can you describe that process?

2 A. Yeah. So each of the items, it was located in the
3 residence and then brought to a central location inside
4 on the main floor, and we — each of the items were
5 brought down.

6 We recorded the information off of it,
7 serial number, identifying information, and then each
8 item was packaged up with this bag for larger items, and
9 they put a string around it and took this wax stick
10 candle thing and a lighter, and they melted wax from the
11 candle on to the string where it was tied on the evidence
12 item.

13 Then, one of the Romanian National Police
14 guys had this stamp or seal they pressed into the wax, so
15 they knew it was sealed by him. And when it was opened,
16 it would break the wax seal.

17 Q. And who was watching this inventory processing?

18 A. I was watching.

19 Q. Who else?

20 A. The Romanian National Police, Nicolescu was
21 standing there with the escort from the Romanian National
22 Police.

23 Q. And what about Special Agent Macfarlane?

24 A. Yes. He was there, also.

25 Q. And were you taking your own notes on each device

Mr. Frost - Direct

1 collected?

2 A. Yes.

3 Q. And what were you recording?

4 A. I was recording the same information, put which room
5 it was located in, and I numbered the items, recorded
6 what the item was and any the identifiable information
7 and the serial number.

8 Q. Okay. And did you sign every page of Government's
9 Exhibit 5?

10 A. Yes.

11 Q. Okay. Can you use the arrow to show us where your
12 signature is on this front page?

13 A. Yeah. That's me, Matthew Frost.

14 Q. Okay. Did Bogdan Nicolescu sign every page of the
15 inventory form as well?

16 A. He did sign after all of us signed.

17 Q. And was Bogdan Nicolescu handcuffed at the time he
18 signed every page?

19 A. He was not.

20 Q. Did you see Bogdan Nicolescu raise any objection to
21 the search or to the inventory?

22 MR. GOLDBERG: Objection.

23 THE COURT: Sustained.

24 BY MR. LEVINE:

25 Q. Did you see Nicolescu threatened by the RNP or

Mr. Frost - Direct

1 anyone else?

2 MR. GOLDBERG: Objection.

3 THE COURT: Sustained.

4 BY MR. LEVINE:

5 Q. What did you see in terms of Nicolescu and his —
6 the time at which he was signing the form?

7 A. He — at this point in time, like I said, the
8 handcuffs had been removed, and he was following us
9 everywhere we went inside the residence, and as we
10 signed, he was there. And then, once we completed
11 signatures, he went to the documents and signed them,
12 also.

13 Q. Okay. Once the RNP had inventoried all the items
14 and in the bags, did they take them away?

15 A. Yes.

16 Q. And before leaving the residence, did Nicolescu do
17 anything?

18 A. Yes.

19 Q. What did he do?

20 A. He — after we had packaged all the items and the
21 Romanian National Police took the items, he went
22 throughout the home with a small bag and collecting some
23 small personal items, like an overnight bag, a shirt and
24 some other items inside this little bag.

25 He was quite methodical on what he decided

Mr. Frost - Direct

1 to take. It took quite a while and went back and forth
2 and seemed like he was trying to decide what to take and
3 not to take for the trip.

4 Q. Okay. And when you got back to the United States,
5 did you make forensic copies of some of the computers,
6 hard drives, and other devices that were seized in
7 Romania?

8 A. Yes.

9 Q. And did you make copies of the devices seized from
10 Nicolescu's house or other devices, too?

11 A. I made copies of both items from Nicolescu's house
12 and other items that had been seized from other locations
13 within Romania.

14 Q. Okay. And I would like to show you what has
15 previously been marked as Government's Exhibit 2045, and
16 I will hand you a hard copy and bring that up. And if
17 you could go to page 2.

18 MR. LEVINE: Thank you so much, Sue. And if
19 we can also go to page 3, page 4.

20 BY MR. LEVINE:

21 Q. Okay. Let's go back to page 2.

22 Does Government's Exhibit — first of all,
23 what is Government's Exhibit 2045?

24 A. This is a certificate of authenticity that I wrote
25 about the devices that I imaged and processed; a little

Mr. Frost - Cross

1 bit of my background, who I am, what I do, my experience,
2 and then the items and how I labeled them and what they
3 were and where they came from.

4 Q. Okay. Does Government's Exhibit 2045 contain a fair
5 and accurate list of all the computers, hard drives, and
6 other devices you made forensic copies of as part of this
7 investigation?

8 A. Yes.

9 Q. And did you make complete and accurate copies of all
10 the digital devices referenced in Government's Exhibit
11 2045?

12 A. Yes.

13 Q. Have all the digital devices you reviewed been
14 returned to Cleveland FBI?

15 A. Yes.

16 Q. And have all the digital copies you created been
17 provided to Cleveland FBI?

18 A. Yes.

19 MR. LEVINE: No further questions for this
20 witness, your Honor.

21 THE COURT: Cross examination, Mr. Goldberg?

22 MR. GOLDBERG: Thank you.

23 CROSS EXAMINATION

24 BY MR. GOLDBERG:

25 Q. Good morning, Mr. Frost.

Mr. Frost - Cross

1 A. Good morning.

2 Q. Couple questions:

3 You were present at the search of this home
4 in Braosov, correct?

5 A. Yes.

6 Q. And do you regularly accompany police officers
7 or the FBI on searches that involve breaching a
8 house or breaking a door down? Do you regularly do
9 that?

10 Is that regularly part of your job?

11 A. Yes. I regularly execute searches —

12 Q. And you do this in the United States, or do you do
13 this outside the United States?

14 A. Both within the United States and outside the
15 United States.

16 Q. So you described the house as having a fence around
17 the outside with an iron gate, correct?

18 A. Yes.

19 Q. Now, that iron gate was open?

20 A. No.

21 Q. So the police had to open the iron gate that was by
22 the street?

23 A. The — when we got to the residence, the gate was
24 closed, and the Romania National Police, I don't remember
25 exactly, but I believe they went up and over the walls to

Mr. Frost - Cross

1 get in because the gate was locked.

2 Q. You don't remember how they got through the gate, or
3 you don't remember whether it was locked?

4 A. I don't remember exactly, but what I do remember,
5 once they cleared and came back, we went through the
6 gate.

7 Q. So you don't know how the gate was opened
8 necessarily?

9 A. Correct.

10 Q. So you entered the house, and you made an inventory
11 of just your own personal inventory of just the
12 electronics, or did you make an inventory of everything
13 in the home?

14 A. I made the inventory of the items that we were going
15 to seize.

16 Q. Okay. Well, there were other items besides
17 electronics that were seized in the search, correct,
18 personal items, credit cards, bank account information,
19 things like that?

20 A. Yes, there were other items. I was present during
21 the search, and my focus was just on the electronic
22 items.

23 Q. Right. You focused on the electronic items, but you
24 signed the search warrant on every page that contains
25 everything that was taken in the search, correct?

Mr. Frost - Cross

1 A. Yes.

2 Q. All right. So prior to this search being executed,
3 were you briefed on this investigation?

4 A. Yes.

5 Q. Were you aware that the house that was going to
6 be searched was rented by someone other than
7 Mr. Nicolescu?

8 A. I don't know who owned or leased or rented the home.
9 All I know is who was in the home when I showed up.

10 Q. You keep saying Mr. Nicolescu's house. That's
11 because that's who was there when you went in,
12 correct?

13 A. Correct.

14 Q. But there was property belonging to other
15 individuals in that house when it was searched,
16 correct?

17 A. I don't know who owned any of the items.

18 Q. Well, let me ask you this:

19 Do you know whose name the internet service
20 connected to that house was in?

21 MR. O'SHEA: Object.

22 THE COURT: Overruled.

23 THE WITNESS: I do not.

24 BY MR. GOLDBERG:

25 Q. Okay. And that wouldn't be part of your

Mr. Frost - Cross

1 investigation. You wouldn't be interested in that?

2 A. So I am not the investigator. I don't do the
3 investigations. I was there solely there in Romania to
4 assist the Romanian National Police execute the search
5 for digital devices.

6 Q. Right. But your job is to secure, search,
7 secure and search the individual electronic devices,
8 correct?

9 A. Yes.

10 Q. And isn't — isn't it relevant what internet service
11 is connected to any of these devices? Isn't that
12 relevant to your inquiry?

13 A. Again, I was there assisting the Romanian National
14 Police with their search warrant. I don't know if they
15 asked for the FBI's assistance or we asked for their
16 assistance.

17 I was asked to come in, and I don't
18 investigate; all I do is identify devices that contain
19 digital storage, and then I assist with their legal
20 process. Again, I don't know Romanian law. I was there
21 assisting the Romania National Police execute their
22 search warrant in their country.

23 Q. So one last question on this: In terms of what you
24 were doing on this case, the source of the internet
25 connection into the house was not important to you. I

Mr. Frost - Cross

1 think that's what you just said.

2 A. I didn't say it was not important to me. We seized
3 all digital devices we felt might contain evidence, and
4 we took the router with us.

5 Q. And the router was connected to an outside internet
6 source, correct?

7 A. I didn't get on the network. I don't know where the
8 source was. I know it was connected to the home.

9 Q. And I am holding up Government's Exhibit 2046. This
10 is the wireless router, correct?

11 A. That is a router. I don't know if it is wireless.
12 I don't see an antenna coming off it.

13 Q. Is this the only router that you seized in the
14 house?

15 A. Without verifying with my notes, I can't compare it.
16 I know that was a router seized from the house.

17 Q. And this router was connected to a cable that
18 supplied, presumably supplied an internet connection,
19 correct?

20 A. Yes. Routers connect two separate networks. So one
21 network connects to another network, and it routes
22 traffic between those two networks.

23 Q. So 2046 had to be connected to an outside source of
24 the internet, correct?

25 A. If it was the router connecting the internet and the

Mr. Frost - Cross

1 home, then, yes, it would have been connected to an
2 internet source.

3 Q. Do you know if this was that one?

4 A. Again, I don't know. We didn't get inside the
5 devices while we were on scene. I just know it was
6 connected inside the home.

7 Q. Okay. What was it connected to?

8 A. Network cables running through various machines that
9 — it was in the kitchen where the HP computer was, and
10 there were other computer cables running outside the home
11 to other parts of the home.

12 Q. Do you know which machines specifically were plugged
13 into this router?

14 A. I do not.

15 Q. Now, you talked about these two larger computers
16 that are on the dolly, Government's Exhibit 2039 and 2038
17 a few minutes ago, correct?

18 A. Yes.

19 Q. So 2038 was the one that has been damaged, and your
20 testimony was, it didn't look like this when it was
21 sitting in the house, correct?

22 A. That is correct.

23 Q. And somehow between Braosov and — let me put it
24 this way: You didn't image this computer at the time it
25 was seized, correct?

Mr. Frost - Cross

1 A. Yes.

2 Q. You did?

3 A. That is correct. I did not image it at the time it
4 was seized.

5 Q. When did you image it?

6 A. It was imaged in Pocatello when I received it in
7 2017.

8 Q. So when you saw it in the house in Brasov in 2016,
9 it was not imaged?

10 A. Correct.

11 Q. Is this the way you usually receive evidence seized
12 by the FBI at your lab?

13 A. So we seize evidence, when we get it to Pocatello,
14 it is usually shipped to us, and every once in a while
15 items are damaged. When I receive them, I inventory
16 them, take pictures just to verify everything before I
17 touch them and start them.

18 Q. But this doesn't look like damage that would have
19 been — would have been normally — would have been
20 associated with a normal inspection of the machine,
21 correct?

22 MR. LEVINE: Objection.

23 THE COURT: Overruled. Can you answer that,
24 sir?

25 A. If you can rephrase.

Mr. Frost - Cross

1 Q. Normally when a machine is seized, it may be
2 disassembled, looked at, the interior may be viewed,
3 right?

4 A. Yes.

5 Q. And that's done using a screwdriver and maybe
6 pliers, other things?

7 A. Yes.

8 Q. It is not normally rolled down a hill, right?

9 MR. LEVINE: Objection.

10 THE COURT: Sustained.

11 BY MR. GOLDBERG:

12 Q. It is not normally beaten up like this —

13 MR. LEVINE: Objection.

14 THE COURT: Sustained.

15 BY MR. GOLDBERG:

16 Q. Does it normally look like this?

17 A. When you say "normally," there is all sorts of
18 different searches that I have been on, and when items
19 are in the control that entire time, it doesn't look like
20 that. I have received computers that have been damaged
21 and broken. I have received several servers from
22 international shipping that, when I received them, the
23 metal frames had been damaged, and there was physical
24 damage that wasn't there when I was in the country?

25 But during the international shipment

Mr. Frost - Cross

1 process, sometime when it wasn't in my custody, damage
2 had been inflicted to the systems.

3 Q. All right. So you were able to image the data that
4 was on 2038, correct?

5 A. Yes. I imaged the drives inside the system.

6 Q. Just the drives?

7 A. Yes.

8 Q. And did you give us a number for the amount of
9 gigabytes total contained of memory, contained in this
10 image?

11 A. Memory like RAM or memory storage on the hard
12 drive?

13 Q. Storage.

14 A. I don't know the exact number without referring to
15 my notes. I imaged them in 2017, January-February time
16 frame. They were, like I said, between 500 gigabytes and
17 a terabyte or two terabytes roughly.

18 Q. And do you know how much storage capacity is
19 required to store, let's say, a high definition feature
20 length movie?

21 A. High definition, Blue Ray, HDVD, there is different
22 definitions of high definition, 720p, 1080p.

23 Q. So you could use up to four to five gigabytes of
24 storage space to store one feature length movie if it is
25 the right type of media.

Mr. Frost - Cross

1 A. On a DVD, yeah, 4.7 gigabytes.

2 Q. 4.5, something like that?

3 A. Yeah.

4 Q. And you imaged the data on this device, 2039, and
5 you indicated that the hard drives were encrypted?

6 A. Yes.

7 Q. Encryption is something that is available —
8 encryption programs are available as a source on the
9 internet?

10 A. Yes.

11 Q. And is there anything illegal about encrypting
12 a machine, a computer that contains a lot of
13 information?

14 A. No.

15 Q. And at the end of the day, you weren't able to image
16 any actual data contained in 2038, Exhibit 2038?

17 A. Image the data, so we imaged all the data. I just
18 couldn't view —

19 Q. From your investigation, you can't say what is on
20 the storage media in this computer?

21 A. Correct.

22 Q. And you are familiar with what was the state of the
23 art in terms of the technology for various computer
24 devices in 2016, correct?

25 A. Yes.

Mr. Frost - Cross

1 Q. So what was the age on this machine, at least on the
2 tower, Government's Exhibit 2038?

3 A. I don't know the age on the tower itself. There was
4 just a black box that is not a Dell or HP that I could
5 look up and see when that model was created.

6 Q. And there is no serial number right on the back of
7 the tower itself right here, can you tell?

8 A. I believe there is a serial number, yes.

9 Q. Did you look up when this particular machine was
10 built?

11 A. I did not.

12 Q. Would you agree with me that the machine, when you
13 saw it, appeared to be several years old?

14 A. The tower itself — are you asking for the age of
15 the tower?

16 Q. I am asking about the age of the tower, if it is
17 brand new?

18 A. The tower itself, I don't know what the age of it
19 is. A black tower, it could be brand new.

20 Q. But you didn't look it up. You don't know?

21 A. No. I have to have a specific model.

22 Q. What about each of the hard drives that were
23 contained inside, 2038, did you look at the age of those
24 items?

25 A. I took off all identifying information from the

Mr. Frost - Cross

1 drives, and I don't recall what year they were, produced.

2 Q. Okay. But none of this technology that we are
3 talking about, specifically 2038 and any of the hard
4 drives that were contained, were cutting edge, up to date
5 items. These were items that had been available in the
6 marketplace for a while, correct?

7 A. Yes. They were available in the marketplace.

8 Q. And there is nothing on this computer, 2038, that
9 was not available freely on the internet or at most
10 computer oriented stores, correct?

11 A. Freely on the internet available to purchase to
12 anyone?

13 Q. I don't mean for free. You can go on the internet
14 and purchase all this?

15 A. Yes.

16 Q. And I could probably go into Comp USA out in
17 Mayfield and pickup all this as well?

18 A. Yes.

19 Q. Okay. Now, you had an opportunity to image the
20 contents of the other large machine, 2039, as well,
21 correct?

22 A. Yes.

23 Q. Was there anything encrypted or unencrypted
24 contained on any of the hard drives in this
25 machine?

Mr. Frost - Cross

1 A. Yes. There was data on the hard drives.

2 Q. Okay. But it was unencrypted?

3 A. Yes.

4 Q. Do you know whether this machine was in recent
5 use?

6 A. I don't know when it was last used.

7 Q. Okay. Was it connected to any other machine when
8 you arrived at the premises?

9 A. I don't recall.

10 Q. Wouldn't that be an important piece of information
11 for this investigation, whether — what you had called a
12 server was connected to another server?

13 A. That's a piece of information I would usually get.
14 Usually, when I enter a search scene, I take pictures or
15 we have a photographer that goes through each room and
16 takes pictures of how we located and what condition it
17 was in.

18 Because I was a guest in Romania and they
19 were lead on the search, they were in charge of the
20 search, and I was a guest in their country. I am not
21 familiar with laws and customs on the legal — to take
22 pictures or not take pictures. So I didn't take any
23 pictures myself. I was just there assisting the
24 Romanians.

25 Q. So your notes don't contain information about

Mr. Frost - Cross

1 connections between machines; only about connections
2 between some of the machines and the router?

3 A. My notes contained identifying information where it
4 was located.

5 Q. Okay. So you've called these servers, and you call
6 them servers because of anything particular with the
7 towers themselves?

8 A. The way they are built and the server grade, Dell.

9 Q. Server grade, Dell. And that's the 2038, right?

10 A. The Dell is the —

11 Q. The second. It is server grade because it has the
12 dual power supplies, correct, among other things?

13 A. Yes.

14 Q. Okay. But you don't know whether or not this Dell
15 was in use at the time that you entered the premises,
16 correct?

17 A. It was powered offline to the residence.

18 Q. All right. But it was also partially disassembled,
19 correct?

20 A. It was disassembled, yes, but you can run drives
21 with them open outside the system.

22 Q. Was it connected to a power source?

23 A. I don't recall.

24 Q. Okay. And this was — this home in Braosov was a
25 regular one-family house, correct?

Mr. Frost - Cross

1 MR. LEVINE: Objection.

2 Q. As far as you know, if you know.

3 THE COURT: Overruled, if you know.

4 A. It was my first time in Romania. It appeared to be
5 a home like you would find in America. I don't know if
6 that's common in Romania or not.

7 Q. I am sorry to use the word "regular." So it looked
8 like a common home to you?

9 A. It was a house.

10 Q. Did you see a generator or any secondary power
11 source?

12 A. I did not.

13 Q. So even though this computer has dual power sources
14 to drive the redundancy, you also need dual power inputs
15 in order for that to make a difference. You need a dual
16 power source, correct?

17 A. Yes. If the grid itself goes down, then you would
18 need a secondary power source to power the computer.

19 Q. And that was not present as far as you know?

20 A. Correct.

21 Q. Now, there is nothing illegal about having a server
22 in your home, correct?

23 A. That's correct.

24 Q. And in fact, the internet is made up of millions of
25 servers, some of which are commercial and some

Mr. Frost - Cross

1 home-based, right?

2 A. Yes.

3 Q. There could be millions of home-based servers all
4 over the world?

5 A. I am not familiar. I haven't been everywhere in the
6 world.

7 Q. All right. But they exist. It is not uncommon to
8 find a server that is not on a server from AOL but at
9 someone's home?

10 A. It is uncommon for me to locate a server outside of
11 a base or data center.

12 Q. And servers are used by companies like — and I am
13 guessing — Netflix probably has their own servers that
14 are accessed when you stream a movie, correct?

15 A. Yes.

16 Q. And that would be like a media server, correct?

17 A. Yes.

18 Q. And there are file servers, which allows access from
19 other machines or from outside on the internet just to
20 view files, correct?

21 A. Yes.

22 Q. And people use, researchers use servers or high
23 capacity computers to solve physics equations if that's
24 what they need to do, correct?

25 A. Yes.

Mr. Frost - Cross

1 Q. Or collate genetic research, correct?

2 A. Yes.

3 Q. And somebody who lives — would you say Brasov
4 was a bustling metropolis or kind of an out-of-the-way
5 place?

6 A. It was removed from Bucharest, the main city, that
7 was smaller, but it was nice.

8 Q. And would somebody be able to use a high capacity
9 machine such as 2038 with all that memory to use for
10 gaming?

11 MR. LEVINE: Objection, your Honor.

12 THE COURT: Sustained.

13 BY MR. GOLDBERG:

14 Q. A person using this machine and the amount of
15 capacity, would they be able to store movies, a number of
16 movies on it?

17 A. Yes.

18 Q. Would they be able to play high definition modern
19 video type games on it?

20 A. The — I would have to check and look at the
21 graphics card. Usually, a graphics card is a component
22 of the system, and gaming machines or the system itself
23 costs a thousand dollars. The graphics cost a thousand
24 dollars because that's where all the computations happen.

25 So if I look at the system, I could look at

Mr. Frost - Cross

1 the graphics card, do some search and see.

2 Q. Did you happen to look to see if there was a
3 graphics card?

4 A. There is a graphics card. I don't recall — there
5 was not a big huge one with lots of memory and multiple
6 fans.

7 Q. But servers are utilized in the gaming world to host
8 and play online games?

9 A. Yes.

10 Q. And some of those games require a lot of data. I
11 know everything is relative, but compared to ten years
12 ago, the games that are now available require much higher
13 capacity?

14 A. Yes, they do.

15 Q. You indicated at some point Mr. Nicolescu was
16 allowed, permitted by the Romania police to contact a
17 lawyer or a trusted friend?

18 A. Yes. They were talking in Romanian. I am not sure
19 what the conversation was.

20 Q. Do you know if Mr. Nicolescu was ever able to
21 contact anyone?

22 A. I again don't know who he talked to or what was
23 said. I know somebody showed up at the residence, and
24 they were talking Romanian. I don't know who that person
25 was.

Mr. Frost - Cross

1 Q. Okay. But eventually, the Romanian National Police
2 were able to proceed?

3 A. Correct.

4 Q. And Mr. Nicolescu, as far as you could tell, didn't
5 object to them conducting their business, doing their
6 work, searching the house?

7 A. That is correct.

8 MR. O'SHEA: I would like to have one
9 moment, your Honor.

10 THE COURT: You may.

11 (Pause.)

12 MR. GOLDBERG: If I may approach?

13 THE COURT: You may.

14 BY MR. GOLDBERG:

15 Q. The government showed you Exhibit 5, was the actual
16 search warrant with the translation.

17 Do you remember seeing that a few minutes
18 ago?

19 A. Yes.

20 Q. And you indicated you signed each page?

21 A. Uh, yes.

22 Q. Okay. And did you actually read each page before
23 you signed it?

24 A. The document that was presented was in Romanian
25 again. The items that I saw serial numbers were items I

Mr. Frost - Cross

1 referenced and recognized.

2 Again, we were guests in their country,
3 and they said because we were adversary at the scene, we
4 had to search the document or sign the document, excuse
5 me.

6 Q. Okay. So you just signed it, but you really didn't
7 know what it said other than the serial numbers?

8 A. Correct.

9 Q. Were you aware when you sign a document
10 that there was a number of items belonging to
11 Mr. Nicolescu, personal items taken in the search, not
12 computers necessarily but things like bank cards or
13 papers?

14 A. Yes. There were items that weren't the digital
15 items.

16 Q. So you noticed that when you signed it. You must
17 have also noticed there were items belonging to
18 Mr. Nicolescu that were taken into the search?

19 MR. O'SHEA: Object.

20 THE COURT: Overruled.

21 A. Again, I don't know who the documents belonged to.
22 I just know they were at the residence.

23 Q. You just said you saw there were personal items,
24 papers taken belonging to Mr. Nicolescu. You said you
25 noticed that before you signed this.

MR. Frost - Cross Cont'd

1 So I am asking, since you noticed
2 Mr. Nicolescu's name, did you notice that Mr. Radu
3 Miclaus's name is also on the search warrant for items
4 taken in the search?

5 MR. O'SHEA: Object.

6 THE COURT: Overruled.

7 A. Again, it was two years ago. I don't remember
8 everything that was on there but I did review the
9 document and then I signed like I was asked to?

10 MR. GOLDBERG: Thank you. Nothing further,
11 your Honor.

12 MR. O'SHEA: One moment, Judge.

13 THE COURT: Certainly.

14 (Pause.)

15 CROSS EXAMINATION CONTINUED

16 BY MR. O'SHEA:

17 Q. Good morning, Agent Frost.

18 A. I am an examiner; not an agent.

19 Q. I'm sorry?

20 A. I am not an agent. I am just an examiner.

21 Q. You are an examiner. I thought you were going to
22 tell me your name wasn't Frost.

23 Thank you for the work that you do for the
24 FBI by the way.

25 Can you tell the ladies and gentlemen of the

MR. Frost - Cross Cont'd

1 jury the difference between cloning and imaging a hard
2 drive. Is there a difference?

3 Let me start with that question.

4 A. Yes.

5 Q. Tell us the difference.

6 A. When you clone a hard drive, you take the hard
7 drive, and you copy it exactly the way it is on the drive
8 and put it on the same size drive, so it is an exact
9 copy.

10 Q. Okay. And IS cloning a more accurate way of getting
11 a copy of a drive than just simply imaging it then,
12 stated it another way.

13 A. When you say a more accurate, are you talking about
14 the clone versus imaging the drive?

15 Q. Yes, sir. The cloning, you have more stuff. It
16 is much more accurate than an image. Am I right about
17 that?

18 A. Well, an image captures the data inside the drive
19 and makes an exact copy, just puts it in a different
20 format.

21 Q. Okay. And how is it different than cloning because
22 cloning has got more data? It is actually like an exact
23 duplicate of the target drive, am I right, cloning?

24 A. So, yes. When you clone it, you copy off all the
25 data and put it back on the same exact the way it was.

MR. Frost - Cross Cont'd

1 When you image it, you take it and put it in a format
2 that — it copies all the data again.

3 It just puts it in a format that compresses
4 things if there is empty space on the drive. Imaging is
5 a more efficient way. I wouldn't say it is a better way.

6 Both times when you clone a drive or when
7 you image a drive, there is a verification process we go
8 through to verify the original matches the copy, whether
9 it is a clone or an image.

10 Q. Okay. But so I understand the technology, the clone
11 is an exact copy of the target drive where the mere image
12 drive is mostly that, but it is more efficient to review
13 it. Am I right about that?

14 MR. LEVINE: Objection.

15 THE COURT: Overruled. Is that correct,
16 sir?

17 THE WITNESS: That was a long question.
18 Can. You repeat that question?

19 BY MR. O'SHEA:

20 Q. Okay. Let me back up.

21 The imaging work that you did, you created a
22 mirror of the drive or a clone drive of these computers
23 that were received?

24 A. I created image copies.

25 Q. Okay. You did not do cloning. Am I right?

MR. Frost - Cross Cont'd

1 A. Correct.

2 Q. You were not tasked with that responsibility. Am I
3 right?

4 A. Yes.

5 Q. Had you been tasked with that responsibility, would
6 you have done it?

7 MR. LEVINE: Objection.

8 THE COURT: Sustained.

9 BY MR. O'SHEA:

10 Q. Now, before one either images or clones a hard
11 drive, any device, cellphone, computer, is it a good idea
12 to shut the device down before any equipment is attached
13 to that computer or device, sir?

14 MR. LEVINE: Objection.

15 THE COURT: Overruled. You may answer
16 that.

17 A. It depends on the type of imaging you are doing and
18 what the original device is and what techniques and
19 methods are available, whether you capture it live while
20 it is on or capture, and some things don't matter whether
21 it is on or off and some things do matter.

22 Q. You correct me if I am wrong.

23 If you don't shut the device down, then
24 while you are attached to it, that computer, the target
25 computer or drive or device is also doing what it

MR. Frost - Cross Cont'd

1 normally does if it is just standing alone. Am I
2 right?

3 MR. LEVINE: Objection, your Honor.

4 THE COURT: Overruled. Did you understand
5 the question, sir.

6 THE WITNESS: Yes. So if a system is on,
7 again, it depends on how many drives, what's connected,
8 what the system is doing. It can be making edits to the
9 original that is there while it is running.

10 Q. Okay. Is that why sometimes the best protocol is to
11 shut the device off before you start any imaging or
12 cloning process?

13 A. Again, it depends on the circumstance.

14 Q. How about in this circumstance?

15 A. In this circumstance, if the computers were on and
16 we were able to access them in an unencrypted state, then
17 we would have imaged them live on scene and captured the
18 data when it was accessible as opposed to imaging when it
19 was turned off, and everything is then encrypted or in
20 the state it was when it is turned off, whether it is
21 encrypted or unencrypted.

22 Q. Okay. Well, you were there that day I gathered from
23 your direct testimony, sir.

24 Were the computers left on or shut off while
25 you were there?

MR. Frost - Cross Cont'd

1 A. Some of them were on; some of them were off.

2 Q. Okay. Were some of them shut off by the agents, or
3 were they already off when you got there?

4 A. Some of them were already off when we got there.

5 Q. Do you know who shut them off?

6 A. No.

7 Q. After you got there, did some of the machines get
8 shut off?

9 A. Yes.

10 Q. And they got shut off, I assume — correct me if I
11 am wrong — they got shut off because they were being
12 seized and cataloged with evidence with the idea at some
13 point they would be imaged.

14 Am I right about that, sir?

15 A. Yes. The Romanian National Police shut everything
16 down we were going to take.

17 Q. Now, when one images or clones a hard drive, hard
18 drives are built into things called sectors. Am I right
19 about that, sir?

20 A. Yes.

21 Q. Okay. And some sectors are more important than
22 other sectors. Am I right about that?

23 A. If you are referring to storing the data or
24 running the system, the data is stored throughout the
25 drive.

MR. Frost - Cross Cont'd

1 Q. Okay. Well, for instance, when you are doing this
2 type of imaging or cloning the important files to
3 extract, are these temporary files, history logs and
4 browser artifacts. Am I right about that, sir?

5 A. It depends on the investigation, but those can be
6 important.

7 Q. How about this investigation?

8 A. Yes. We would like to have had those.

9 Q. And it is also important to get registry files and
10 system metadata. Am I right about that?

11 A. If you are talking about windows registry, then,
12 yes, you would find a registry on a windows system, a
13 Linux system.

14 Q. And what is a blocker device, sir? That is
15 referenced, I believe, in one of the exhibits that you
16 looked at. What's a blocker?

17 A. Are you referring to a write blocker?

18 Q. Well, I think — you were asked questions about
19 Exhibit 2045, which is a certificate of authenticity. Do
20 you remember that line of questioning, sir?

21 A. Yes.

22 Q. Okay. And on paragraph 7, there is something called
23 a write blocker. Tell us what a write blocker is in the
24 context of that document, sir.

25 A. Yeah. So a write blocker is, that is a standard

MR. Frost - Cross Cont'd

1 operating procedure. When we are able to image a drive
2 and it is not powered off, we will connect it to a
3 separate device that we performance verify, and this
4 device, it is a one-way traffic device.

5 So we are able to read the data off the
6 drive. We are not able to write data back to the drive.
7 That's why it is a write blocker. It blocks all writes.

8 And all of my equipment each year, we
9 performance verify that all the drives won't allow writes
10 to go on to the evidence drive and only allow one way
11 data from the original to the copy.

12 Q. Okay. And as part of the extraction process when
13 you are doing forensic evaluations of computers
14 generally, can you actually determine whether a computer
15 has a thing called a cookie on it?

16 A. Can I — if the cookie is there and I am able to
17 read the drive and locate it, then, yes, I can determine
18 if there is a cookie on the drive.

19 Q. Tell us what a cookie is.

20 A. Cookies are left by — when you do internet
21 browsing, it will leave a cookie on your system, and that
22 this is one way a website can track you've been there.
23 It stores some of the information, knows you have been
24 there before.

25 Q. So if I have a computer at home or my wife or

MR. Frost - Cross Cont'd

1 children do and they go to an internet site like
2 Yahoo, Facebook, without that, that is temporarily
3 planting files on their computer so it can track them,
4 right?

5 MR. LEVINE: Objection, your Honor.

6 THE COURT: Overruled. You may answer.

7 A. Depending on the browser setup. Some browsers are
8 set up so it won't store cookies. Some are set up if you
9 visit a website by using the producer, you are using and
10 accessing their website, and the cookie is dropped on
11 your machine.

12 Q. Unless you have the ability to change the settings
13 on your browsers, unless you know to set them in a
14 certain way, those cookies will be planted on your
15 computer without your permission, am I right?

16 MR. LEVINE: Objection, your Honor.

17 THE COURT: Sustained.

18 BY MR. O'SHEA:

19 Q. And I think Mr. Goldberg went over this a little
20 bit, too. Large hard drives or multiple hard drives
21 themselves are not illegal, right?

22 A. Correct.

23 Q. As a matter of fact, they are very common in the
24 music and movie industry in order to store large amounts
25 of data. Am I right?

MR. Frost - Cross Cont'd

1 MR. LEVINE: Objection, your Honor.

2 THE COURT: Overruled.

3 A. So if you are talking a movie industry that's
4 producing content, they probably have massive evasive
5 storage.

6 Q. Okay. And that's not illegal, right?

7 A. Correct.

8 Q. And same with music, people like Pandora and stuff
9 like that, they have to have massive hard drives to store
10 all their information. Am I right about that?

11 A. Yes.

12 Q. And I think Mr. Goldberg went through it, encrypted
13 devices, be they phones, be they laptops, desktops,
14 servers are not illegal, right?

15 A. In the United States, no.

16 Q. And just so we are clear, I think this same
17 document, 2045 that you have in front of you, sir, in the
18 first paragraph of that document, you make reference to
19 the fact that you have been involved with about 6,000
20 imaging tasks. Am I right about that?

21 A. Yes.

22 Q. Now, as it relates to these specific items here on
23 this cart, the exhibits we heard them and again, 2046,
24 2039, 2038 and the others, you don't specifically
25 remember these devices, where they were or anything from

MR. Frost - Cross Cont'd

1 your own memory given that you have done 6,000 of these
2 things.

3 You relied on reviewing documents and
4 preparing for your testimony here this morning. Am I
5 right, sir?

6 A. Usually, that's correct. I do remember specifically

7 —

8 Q. The dented one?

9 A. The Dell server because the drives were out, and I
10 guess it is just vivid that I remember that.

11 Q. Other than that, without the assistance of the
12 paperwork that has been supplied to you, it would be
13 unfair to you in light of the volume you do for you to
14 remember everything about this particular case. Am I
15 right about that?

16 MR. LEVINE: Objection, your Honor.

17 THE COURT: Overruled.

18 A. Correct. I take notes and review later and document
19 my process.

20 Q. And you take the notes, so if it comes to tasks like
21 this, you are able to refresh your recollection. Am I
22 right about that?

23 A. Yes.

24 Q. And last couple inquiries, sir, or maybe just one
25 depending on your answer.

MR. Frost - Cross Cont'd

1 As you sat there this morning, you indicated
2 to us that you don't know — that you personally have no
3 idea who owned what at that house that day. Am I right
4 about that?

5 A. Correct. I don't know who owned it. All I know is
6 who was there when we arrived.

7 MR. O'SHEA: Thank you. Nothing further,
8 Judge.

9 THE COURT: Redirect?

10 MR. LEVINE: No redirect, your Honor.

11 THE COURT: You may step down, sir. Watch
12 your step. Do you want to call another witness at this
13 point?

14 MR. LEVINE: May we approach, your Honor.

15 (Discussion held off the record.)

16 THE COURT: Ladies and gentlemen we are
17 going to take our luncheon recess. Please remember the
18 admonition. Please be downstairs at 1:00 o'clock. All
19 rise for the jury.

20 (Luncheon recess taken.)

21 - - - - -

22

23

24

25

Mr. Tiberiu Danet - Direct

AFTERNOON SESSION

THE COURT: Please seated. Please call your next witness.

MR. BROWN: Thank you, your Honor. The United States calls Tiberiu Danet.

THE COURT: Sir, if you would please — I will ask you to stand again, I'm sorry. Please raise your right hand.

TIBERIU DANET

called as a witness by and on behalf of the Government, being first duly sworn, was examined and testified as follows:

THE WITNESS: Yes, I swear.

THE COURT: Please take a seat. Now, you may begin.

DIRECT EXAMINATION

BY MR. BROWN:

Q. Thank you, your Honor. Would you please state your name, and spell it for the court reporter?

A. My name is Tiberiu Danet, T-i-b-e-r-i-u, D-a-n-e-t.

Q. If I could ask you just when you answer to speak loudly and also fairly slowly?

A. Yes.

Q. Thank you. And where were you born, Mr. Danet?

A. I was born in Romania in Bucharest.

Mr. Tiberiu Danet - Direct

1 Q. And up until 2016, where did you reside?

2 A. In Bucharest in Romania.

3 Q. How old are you?

4 A. I am almost 34 next month.

5 Q. Okay. And how far have you gotten in
6 school?

7 A. I have earned a Master's Degree.

8 Q. In what?

9 A. Computer science.

10 Q. Now, what is your high school experience? Did you
11 go to school year?

12 A. International computer in high school, Bucharest.

13 Q. Is that a private high school?

14 A. Private high school.

15 Q. And did it specialize in any field?

16 A. The class I went to was a class where all the
17 students got scholarships for different subjects like
18 some in mathematics, some in biology, some in computer
19 science.

20 Q. And what was your scholarship in?

21 A. Well, I first started when I finished the eighth
22 class, I was within mathematics, so I got into
23 mathematics. They gave me a scholarship for mathematics
24 but eventually, I started to study computer science.

25 Q. Okay. And was this a hard school to get in? Was it

Mr. Tiberiu Danet - Direct

1 difficult?

2 A. I wouldn't say necessarily. I don't know if anybody
3 really wanted to — the way they work, they would pick
4 the students they wanted.

5 Q. So it was selective?

6 A. Yes.

7 Q. Now, while you were there, did you participate in
8 any extracurricular activities?

9 A. Yes. That's how actually they would provide the
10 professors, from like the state high schools would come
11 there and teach you outside of class, the specific
12 subject you are studying.

13 Q. Okay. And did you take any of those specialty
14 subjects?

15 A. Yes, mathematics and computer science program.

16 Q. And were there any, like, school teams or activities
17 surrounding computer science?

18 A. Yes.

19 Q. And did you participate in those?

20 A. Yes.

21 Q. What activity did you do?

22 A. Well, I forgot how many hours a week but probably
23 like eight, at least eight hours a week, somebody, like I
24 said, some professor or maybe somebody that had just
25 finished high school and was very good at computer

Mr. Tiberiu Danet - Direct

1 science would come teach.

2 Q. Okay.

3 A. So most of the programming and coding.

4 Q. And were there any competitions or activities
5 surrounding coding or programming?

6 A. Yes. Everybody was training to go to the national
7 contests for what they are called Olympiad National for
8 math.

9 Q. And did you go to the National Olympiad?

10 A. Yes, every year from ninth to twelfth grade.

11 Q. And would your team represent the school or city, or
12 how would that work?

13 A. First, you represent — there would be different
14 stages. First, you go and are competing against students
15 from the same city. And then, if you qualify to the next
16 phase, the national phase, you go there, and there would
17 be further — then you could qualify for a team, a select
18 team of select students that would go on to represent
19 Romania.

20 Q. And is it fair to say you got to know the guys you
21 were on the national team that you were with?

22 A. Yes. Everybody pretty much new each other like the
23 best.

24 Q. Was Bogdan Nicolescu on your team?

25 A. I met him there when I was in the ninth grade, he

Mr. Tiberiu Danet - Direct

1 was three years older, so twelfth grade.

2 Q. So you got to know him is it fair to say when you
3 were doing your Olympiad?

4 MR. GOLDBERG: Objection.

5 THE COURT: Sustained, sustained.

6 BY MR. BROWN:

7 Q. Is that the first time you met Bogdan Nicolescu?

8 A. Yes.

9 Q. How would you describe your relationship as
10 teammates?

11 A. Nothing special. I mean, just we just talked about
12 the subjects. He had the subjects, and he was given
13 those that were much harder than mine. There probably
14 were 20 —

15 MR. GOLDBERG: Objection.

16 THE COURT: One moment. Next question.

17 BY MR. BROWN:

18 Q. Yes. So you got to know him on the Olympiad team?

19 A. Yes.

20 Q. Approximately what year was this?

21 A. 1999 if I am not mistaken.

22 Q. So you graduated high school in 2003?

23 A. Yes.

24 Q. And from 1999 to 2003, did you maintain contact with
25 Mr. Nicolescu?

Mr. Tiberiu Danet - Direct

1 A. No.

2 Q. What did you do upon graduating from high
3 school?

4 A. I went to college, university.

5 Q. What college?

6 A. University of Bucharest faculty of mathematics and
7 informatics.

8 Q. And by informatics, what do you mean by that?

9 A. It is a term used for computer science.

10 Q. And when did you graduate college?

11 A. 2007, and then I did a Master's Degree for three
12 years more in the same university.

13 Q. Okay. And in the same field?

14 A. Databases.

15 Q. And what do you mean by databases?

16 A. It is a term for holding different kind of data.

17 Q. Is it a field within computer science?

18 A. Yeah, it is a field.

19 Q. So it is sort of a subspecialty of a larger
20 computer —

21 A. Yeah, subspecialty.

22 Q. And what sort of information is taught in a
23 databases course of study?

24 A. How to structure a database, relationships between
25 how to build the database tables, relationships within

Mr. Tiberiu Danet - Direct

1 tables that hold data, how to best structure one, how to
2 optimize it, how to search a database and so on.

3 Q. Is it fair to say, in general, it is accessing and
4 organizing data?

5 A. Yes.

6 Q. Now, while you were at college, did there come a
7 time when you reacquainted yourself with Mr. Nicolescu?

8 A. Yes. It was — I can't remember the year.

9 Q. Were you in graduate or an undergraduate program?

10 A. So undergraduate before the Master's. I am not
11 familiar with the term.

12 Q. Yes. I'm sorry.

13 Was it before you graduated college or when
14 you were in your Master's program?

15 A. It was before I graduated college.

16 Q. Okay. And how did you meet him again?

17 A. He was also a classmate during high school with my
18 brother, so they would sometimes meet each other. I
19 think I just went out with my brother once, and that's
20 when I met him again.

21 Q. And do you recall that first time you met him?

22 A. Excuse me?

23 Q. Do you recall the first time you met him while you
24 were in college?

25 A. It has been — it has been a long time. I don't

Mr. Tiberiu Danet - Direct

1 know.

2 Q. Do you recall the circumstances, not the date
3 necessarily?

4 A. Yeah. I remember he gave me a ride in his car that
5 he had at that time.

6 Q. Okay. Do you recall what kind of car it was?

7 A. It was a BMW, M5.

8 Q. And this was when you were an undergrad. Is that
9 correct?

10 A. Yes, yes.

11 Q. So he would have been a few years older than you?

12 A. Yeah. He is three years older.

13 Q. Are you familiar with cars?

14 A. Yes.

15 Q. Were you impressed by the BMW, M5?

16 MR. GOLDBERG: Objection.

17 THE COURT: Sustained.

18 BY MR. BROWN:

19 Q. You said he gave you a ride. Do you recall where
20 you went?

21 A. Just around town, around Bucharest.

22 Q. Do you know if at that time he was working?

23 A. I don't know.

24 Q. Do you know at that time if he was in college?

25 A. I know that he dropped out of college after — in

Mr. Tiberiu Danet - Direct

1 his first year, after his first year.

2 Q. After you went on this ride with him, did there come
3 a time when you saw him again?

4 A. Yeah, pretty much. I can't remember. It was like a
5 social, either we went out to eat or something —

6 Q. Okay. And do you recall, would you talk together
7 when you went out to eat?

8 A. Well, obviously, I was impressed compared to me,
9 yeah, like with his car and everything, and we started
10 talking about what he was doing.

11 Q. And what did he say he was doing?

12 A. Well, he didn't — he didn't tell me exactly what he
13 was doing, but since he knew me from — before he knew
14 that I was good at programming, and we started talking
15 about like what I been doing in the meantime.

16 Then he proposed that I do something for him
17 on the website.

18 Q. What sort of things did he propose you do for
19 him?

20 A. He said he needed a website, and that he could pay
21 me for it if I could do it for him.

22 Q. And at that time when you were in college, did you
23 know how to design websites?

24 A. Yes.

25 Q. Did you know how to program computers?

Mr. Tiberiu Danet - Direct

1 A. Yes.

2 Q. Did you have specific programming knowledge?

3 A. Yes.

4 Q. What sorts of knowledge did you have about
5 programming computers?

6 A. Well, obviously, what you needed for the national
7 contest, I had been talking about where I done pretty
8 good. You had to know algorithms. You had to know
9 programming languages, maybe C, or they had Pascal back
10 then, and then during — in college, I learned whether by
11 myself or from the courses a little bit of web design,
12 web programming, databases.

13 Q. While you were in college for the graduate program,
14 did you have any internships?

15 A. I did an internship at Google in 2006.

16 Q. Okay. And when you interned at Google, did you go
17 to California?

18 A. Yes, in California.

19 Q. How long was that Google internship?

20 A. Lasted for three or four months.

21 Q. And what sorts of things did Google —
22 generally speaking, what sorts of things did you
23 do at Google?

24 A. We had to follow — you had like a mentor, and he
25 would give you the assignment for that internship, and

Mr. Tiberiu Danet - Direct

1 last three or four months. I worked on something
2 involving pattern matching.

3 Just a simple example, they were working on
4 things like when you search for a person's name, that is
5 a famous person's name, you say when was this person
6 born, it would give you the result, the year, or when did
7 this person die, or you know, in Google, you prompt the
8 results, and they also have some written specific
9 answers.

10 Q. So you were working on search engine type
11 matters?

12 A. Yes, in a sense.

13 Q. So is it fair to say it was about finding data and
14 returning data —

15 A. Yes.

16 Q. — over multiple databases?

17 A. Yes. Somebody already worked on that, and I was
18 following up with his work.

19 Q. Now, going back to Mr. Nicolescu, so he asked you to
20 design a web page?

21 A. A website.

22 Q. Okay. What — what did he ask you to design, what
23 specifically?

24 A. Escrow website.

25 Q. A NASCAR?

Mr. Tiberiu Danet - Direct

1 A. Escrow.

2 Q. Oh, Escrow. I'm sorry?

3 A. Yes.

4 Q. Did he describe to you what he expected the website
5 to do?

6 A. Yes. He gave me pretty detailed specifications, not
7 on how it looked but what the purpose of the website
8 would be.

9 Q. The functionality?

10 A. Yes, the functionality.

11 Q. And what did he want the functionality to be?

12 A. Basically, it would serve as a — it would show the
13 users that wanted to buy specific vehicles. I mean, the
14 scope of it was — the purpose was —

15 MR. GOLDBERG: Objection.

16 THE COURT: Sustained.

17 BY MR. BROWN:

18 Q. Did he give you direction on how he wanted the page
19 to function? I will take small steps here?

20 A. Yes. People would sign up, and they would be given
21 a link, and then, by following that link, they would be
22 able to see some seller's vehicle information, and then
23 they would be able to buy this vehicle by placing money
24 in an escrow account.

25 Q. So an escrow account is an account that holds

Mr. Tiberiu Danet - Direct

1 money —

2 A. The website would hold the money.

3 Q. Okay. And as part of the escrow account, did you
4 have to link it to a sale site, or was it a standalone
5 website?

6 A. No. It was a standalone website.

7 Q. Okay. And did he at that time tell you he was in
8 the escrowing business?

9 MR. GOLDBERG: Objection.

10 THE COURT: Sustained.

11 BY MR. BROWN:

12 Q. Did he tell you this website was for a business of
13 his?

14 MR. GOLDBERG: Objection.

15 A. No.

16 THE COURT: Sustained.

17 BY MR. BROWN:

18 Q. Do you know why or did you, in fact, make the escrow
19 website?

20 A. Yes, I did make.

21 Q. Okay. Did he pay you for it?

22 A. Yes.

23 Q. How much did he pay you?

24 A. Around \$2,000 Euros.

25 Q. Was that a lot of money to you at that time?

Mr. Tiberiu Danet - Direct

1 MR. GOLDBERG: Objection.

2 THE COURT: Overruled.

3 THE WITNESS: Yes, a lot of money. For
4 example I —

5 MR. GOLDBERG: Objection.

6 THE COURT: Sustained.

7 BY MR. BROWN:

8 Q. Did you have a job at that time?

9 A. I had a job before working part-time, small software
10 company, and I was making 400 Euros a month working four
11 hours a day.

12 Q. And how long did this website take you to make?

13 A. A couple of days, maybe a week.

14 Q. So 2,000 Euros for one week worked?

15 A. Yes.

16 Q. Okay. Did you ever see the escrow site work?

17 A. Yes.

18 Q. Do you know — do you know if this escrow website
19 was put on the internet?

20 A. Yes, it was.

21 Q. Okay. And was it linked to other eCommerce
22 sites?

23 A. No. It was a standalone website.

24 Q. When you made that escrow site, what was your
25 understanding of who the clients were? Who was using

Mr. Tiberiu Danet - Direct

1 it?

2 MR. GOLDBERG: Objection.

3 THE COURT: Overruled.

4 A. People wanting to buy vehicles.

5 Q. Okay.

6 A. So it was designed only for vehicles, nothing
7 else.

8 Q. And did you know Mr. Nicolescu to have vehicles he
9 was selling?

10 MR. GOLDBERG: Objection.

11 THE COURT: Sustained.

12 BY MR. BROWN:

13 Q. Do you know if Mr. Nicolescu was working with
14 somebody who was selling vehicles?

15 MR. GOLDBERG: Objection.

16 THE COURT: Sustained.

17 BY MR. BROWN:

18 Q. Did Mr. Nicolescu ask you to do any additional work
19 after that?

20 A. Yes. Eventually, we started talking — I mean, I
21 had a rough idea. He started confiding in me. It was
22 not like he first told me about the escrow website or
23 anything. He didn't tell me anything more.

24 So I knew it was about people usually from
25 America because the website had —

Mr. Tiberiu Danet - Direct

1 MR. GOLDBERG: Objection.

2 THE COURT: Overruled. Go ahead, sir.

3 A. — a state and a city section, so there was no
4 like, if you signed up on their website, you couldn't —
5 or I don't remember exactly, but I don't know if you
6 could have chosen another country besides the
7 United States.

8 Q. Okay. Did you design the website to be just for
9 American clients?

10 A. That's what I remember. It has been a long time
11 though, but, yes.

12 Q. And is that — was that in response to
13 Mr. Nicolescu's request that you make the website look
14 like that?

15 A. Yes.

16 Q. Did he tell you that the website was just to be for
17 cars?

18 A. Yes.

19 Q. Okay. What was the next job he had you do?

20 A. Well, eventually, he started talking to me more
21 about what he was doing for money. The next job —
22 again, it has been a long time. I can't remember
23 exactly the next job — but I remember that I made a
24 website for digital cameras, that supposedly sold digital
25 cameras.

Mr. Tiberiu Danet - Direct

1 Q. Was Mr. Nicolescu selling digital cameras?

2 MR. GOLDBERG: Objection.

3 THE COURT: Sustained.

4 BY MR. BROWN:

5 Q. Did you create the website for a business

6 Mr. Nicolescu asked you about or said that he needed a
7 website for?

8 MR. GOLDBERG: Objection.

9 THE COURT: I am going to sustain that. You
10 will have to rephrase.

11 MR. BROWN: Okay.

12 BY MR. BROWN:

13 Q. Mr. Nicolescu asked you to make another website,
14 correct?

15 A. Yes.

16 Q. Was it a website similar to the one you had made to
17 receive payments for items?

18 A. No.

19 Q. No. What sort of website was it?

20 A. People who just entered their credit card
21 information to buy digital cameras.

22 Q. Was this a website Mr. Nicolescu owned?

23 MR. GOLDBERG: Objection.

24 BY MR. BROWN:

25 Q. Did he say this was for a website he owned, or did

Mr. Tiberiu Danet - Direct

1 you do this —

2 A. No.

3 Q. — acting as contractor —

4 MR. GOLDBERG: Objection.

5 THE COURT: Sustained.

6 Q. — in processing payment — okay.

7 So the website you made processed payments,
8 correct?

9 A. No, it didn't.

10 Q. What did it do?

11 A. It just read the payment information and added to a
12 text file.

13 Q. So it would take credit card information and add it
14 to a text file?

15 A. Yes.

16 Q. Did it ever process a payment?

17 A. No.

18 Q. Okay. When you made the website for the
19 automobiles, did you — was that the same thing? Did it
20 just add the money to a text file, or what happened with
21 that?

22 MR. GOLDBERG: Objection.

23 THE COURT: Sustained.

24 BY MR. BROWN:

25 Q. Okay. What do you mean "adding credit card data to

Mr. Tiberiu Danet - Direct

1 a text file"?

2 A. Just adding it to sort of simple data. You just —
3 again, you would have a summary of all the credit card
4 information entered in the website.

5 Q. So did you pass the credit card information on to —
6 did the website that you designed pass the credit card
7 information on to a camera store?

8 MR. GOLDBERG: Objection.

9 THE COURT: Sustained.

10 BY MR. BROWN:

11 Q. Did you design the website to pass the credit card
12 information on to a camera store?

13 MR. GOLDBERG: Objection.

14 THE COURT: Overruled.

15 A. No.

16 Q. Did the website you designed have any connection to
17 a retail store?

18 MR. GOLDBERG: Objection.

19 THE COURT: Overruled.

20 A. No.

21 Q. Were you told to design a website that was able to
22 connect to a retail store?

23 A. No.

24 Q. Were you told in the original escrow job to connect
25 the escrow web page to a bank?

Mr. Tiberiu Danet - Direct

1 MR. GOLDBERG: Objection.

2 THE COURT: Overruled.

3 A. No.

4 Q. Were you told to design the escrow web page to
5 connect to an auto dealer?

6 A. No.

7 Q. Based on what you were told to do on either of those
8 websites, did you design a website capable of engaging in
9 any eCommerce?

10 MR. GOLDBERG: Objection.

11 THE COURT: Specifically his website?

12 MR. BROWN: Correct, the two he designed.

13 THE COURT: Overruled.

14 THE WITNESS: No. Didn't connect to
15 anything, none of those.

16 THE COURT: Overruled.

17 BY MR. BROWN:

18 Q. Did those two websites you designed collect payment
19 data or credit card data?

20 A. Just the camera one, the digital camera one.

21 Q. Did you ever ask Mr. Nicolescu what kind of business
22 he was engaging in that would require those two types of
23 websites?

24 MR. GOLDBERG: Objection.

25 THE COURT: Overruled.

Mr. Tiberiu Danet - Direct

1 A. No. I didn't have to. Eventually, he told me
2 himself.

3 Q. What did he tell you?

4 A. Well, he started talking about cars being sold on
5 eBay, collecting the money, basically teaching me what he
6 was doing up to the amount.

7 Q. When he started talking to you about the topics,
8 what was your reaction, if anything?

9 A. I was just impressed with the money he was making.

10 Q. So he kept paying you money?

11 A. He paid me money, but I was impressed with the money
12 he had made so far to be able to afford the car, for
13 example.

14 Q. How much money did he tell you he was making?

15 A. He didn't tell me how much he was making. I know
16 that car was worth like \$20,000.

17 Q. And did he describe what he was doing? Like did he
18 have a phrase for what he was doing?

19 A. No. He didn't have one phrase to sum it up.

20 Q. Okay. Based on what you knew, your two websites you
21 designed were doing, did you think there was any
22 legitimate commerce being transacted?

23 MR. GOLDBERG: Objection.

24 THE COURT: Sustained.

25

Mr. Tiberiu Danet - Direct

1 BY MR. BROWN:

2 Q. Did he ask you to make any more web pages?

3 A. Eventually, yes, but I don't remember if it was at
4 that point.

5 Q. What sort of web pages did he eventually ask you to
6 make?

7 A. Web page that looked like the log-in page of Yahoo,
8 AOL, Facebook, Google, modifying a website that looked
9 like work-from-home website, basically trying to hire
10 people to work from home. I can't remember anything else
11 right now.

12 Q. Now, do you remember approximately what year that
13 would have been when he was talking to you about these
14 other types of websites?

15 A. This was late in 2012, '13.

16 Q. Okay. So between 2007 when you met him again, when
17 you were in college, and 2012, you just made two
18 websites?

19 A. No. I did more than that. I mean — no.

20 Q. So let's go back to 2007. You make those two
21 websites.

22 A. Yeah.

23 Q. What's the next thing you do for him?

24 A. Eventually, he told me the scheme he was involved in
25 for making money.

Mr. Tiberiu Danet - Direct

1 Q. And how did he describe that scheme to you?

2 A. It was like a classical eBay fraud.

3 Q. Upon hearing that, what was your reaction, if
4 anything?

5 A. I was interested in it because I knew he was making
6 a lot of money.

7 Q. What sorts of things did he ask you to do to go
8 along with the classic eBay fraud?

9 A. Well, for example, the web page for the digital
10 cameras was needed for the credit cards, so he could
11 create with —

12 MR. GOLDBERG: Objection.

13 THE COURT: Overruled.

14 BY MR. BROWN:

15 Q. Did you help him create web pages that would collect
16 credit card data?

17 A. Yes.

18 Q. Did you help him create pages that would organize
19 the credit card data?

20 A. Yes.

21 Q. Did you help him create web pages that would then
22 access that credit card data?

23 A. No. The information was used —

24 MR. GOLDBERG: Objection.

25 THE COURT: Sustained.

Mr. Tiberiu Danet - Direct

1 BY MR. BROWN:

2 Q. Okay. What sorts of functionality did he ask you to
3 help him create for these frauds?

4 A. I hadn't really created any functionality at the
5 beginning. I was just following his steps for doing the
6 exact thing he was doing.

7 The only thing that was required were credit
8 card information, and that was the reason that he wanted
9 the digital cameras website.

10 Q. Now, were you doing the same thing with automobiles?

11 MR. GOLDBERG: Objection.

12 Q. Did he have you create pages for any other items
13 other than digital cameras?

14 A. No.

15 Q. Okay. So that first escrow website you had designed
16 for him, did he do anything like that with you in 2007
17 again?

18 A. I don't understand the question.

19 Q. Okay. Were there any other frauds he was having you
20 help with other than the digital camera and credit card
21 fraud?

22 MR. GOLDBERG: Objection.

23 THE COURT: Overruled.

24 A. Help him, no. Eventually, he showed me the eBay
25 scheme.

Mr. Tiberiu Danet - Direct

1 Q. And what do you mean by that? What did he show
2 you?

3 A. The steps that you would need to take to make money
4 from trying to sell vehicles that were non existent.

5 Q. Okay. and do you recall approximately what year he
6 showed you those steps?

7 A. It was shortly after the escrow website.

8 Q. Okay. Sometime in 2007?

9 A. I would say so.

10 Q. And what were the steps he showed you?

11 A. The first step would be to create an account with
12 eBay, and for that you needed a credit card. Then, you
13 would list an ad, create a listing with eBay for a
14 vehicle, and the details for that listing you would get
15 from an actual expired listing.

16 Then, people started inquiring about the
17 car. For that, you had to list at a very low price, so
18 something maybe half of the price of the actual car, and
19 then, you would have to contact the interested buyers
20 from an e-mail and tell them that, even though the
21 listing on the website might have ended already, that the
22 car is still available, and they can still buy it.

23 Then, you would give them an account for a
24 third person that resided in America saying that either
25 it is you or you are away on a trip, and that they would

Mr. Tiberiu Danet - Direct

1 get the vehicle after they send the money to that
2 respective account. If they did, obviously, they would
3 not receive — this is where the escrow website would
4 come in handy because you tell them that that account is
5 actually an escrow account, and that the money would be
6 held safely until they got the vehicle.

7 Q. And upon hearing those steps, were you — did you
8 agree to work with him?

9 A. I did.

10 Q. Okay. And at that point, you knew that you would be
11 engaging in eBay fraud?

12 A. Yes, I did.

13 MR. O'SHEA: Objection.

14 THE COURT: Overruled.

15 BY MR. BROWN:

16 Q. Because at that time, you did not have cars to sell
17 on eBay, correct?

18 A. No.

19 Q. And at that time, you understood that the car
20 information was coming from expired sites?

21 A. Yes.

22 Q. So you knew that those were not real cars,
23 correct?

24 A. Yes, I did.

25 Q. Now, when you said you needed the credit card

Mr. Tiberiu Danet - Direct

1 information, where did you get the credit card
2 information to open the account?

3 A. At first or even after that, you could buy credit
4 card information for like \$3 or \$5 apiece, but with that
5 website, you didn't need that if it worked because it
6 didn't always work.

7 Q. And which website are we talking about?

8 A. The digital camera website for collecting credit
9 card information.

10 Q. And that's the one you made, correct?

11 A. Yes.

12 Q. And so you would go through the process of creating
13 an eBay listing?

14 A. Yes.

15 Q. And where did you get photos for those listings?

16 A. From an actual listing from eBay.

17 Q. So you would have to go on to eBay and copy and
18 paste?

19 A. Copy pictures, the description, add to the
20 description, add ons and so on.

21 Q. And same with the detail, right, the listing
22 information?

23 A. Yeah.

24 Q. And where would you get the names to use or the
25 seller's name and seller's location?

Mr. Tiberiu Danet - Direct

1 A. You just make it up.

2 Q. Okay. And how would you find somebody in America to
3 accept a payment to send you?

4 A. First, I wasn't aware of how that happened. I just
5 — Nicolescu would have somebody that would have such
6 accounts.

7 MR. GOLDBERG: Objection.

8 THE COURT: Overruled.

9 Q. Now, was that a labor intensive process?

10 MR. GOLDBERG: Objection.

11 Q. Were there a lot of —

12 THE COURT: Sustained.

13 Q. Were there a lot of steps you have to take to sell a
14 fake car?

15 MR. GOLDBERG: Objection.

16 THE COURT: Sustained.

17 BY MR. BROWN:

18 Q. Every time you wanted to list a car, did you have to
19 go through each of those steps step by step?

20 A. Yes.

21 Q. So each time you wanted to list a car on eBay, you
22 had to go out into eBay and find a photo?

23 A. Yes. You have to first choose a car that you
24 thought looked nice and list, create the account, and
25 list it? Yeah, it took a lot of time.

Mr. Tiberiu Danet - Direct

1 Q. About how much time did it take to make a listing at
2 that point in time in 2007?

3 A. I don't know, say —

4 MR. GOLDBERG: Objection.

5 THE COURT: Sustained.

6 A. — half an hour.

7 Q. Okay. Did you and Nicolescu ever talk about
8 changing that process?

9 MR. GOLDBERG: Objection.

10 BY MR. BROWN:

11 Q. Did you and Nicolescu ever have conversations about
12 the fraud scheme?

13 A. Yes, starting from the beginning when he showed it
14 to me.

15 Q. And based on those conversations, did you do
16 anything to change the fraud scheme?

17 A. Eventually, yes, but — eventually later not in
18 2007.

19 Q. Okay. When? When would these changes have been
20 made?

21 A. When he decided that this classic scheme isn't
22 enough, and it would be — to look much better if the
23 users would see an actual listing on eBay, and let me
24 explain that.

25 I forgot to say, to tell you a step, the way

Mr. Tiberiu Danet - Direct

1 you originally make the buyers send the money was to send
2 an e-mail that was actually a fake e-mail looking like it
3 came from eBay, but this — I mean, people could see that
4 it was not actually from eBay.

5 They would look at the address, so it was —
6 some people would not send the money because they didn't
7 trust the sender — but eventually, we took it to a step
8 where they would be able to see if they would go on their
9 computer on eBay.com, there was a way to get to a listing
10 that looked exactly how we wanted it to look, so it
11 looked very authentic.

12 Q. And what was that process? How did that happen?
13 What was that process?

14 A. We started with making a virus or Trojan that would
15 be installed on the victim's computer. Actually, it was
16 sent by e-mail, and whoever ran it would get infected
17 with this Trojan, and this Trojan would allow us to make
18 a listing that looked authentic right on eBay's website,
19 even if it was not on eBay's website.

20 Q. And who wrote that Trojan?

21 A. Nicolescu.

22 Q. He created the Trojan?

23 A. Yes.

24 Q. Did you help?

25 A. Some parts.

Mr. Tiberiu Danet - Direct

1 Q. Okay. And how would the Trojan get on to a victim's
2 computer?

3 A. Instead of when people would contact you like you
4 still have to list an original car advertisement on eBay
5 and when people contacted you for it, you just send them
6 a link or attachment containing that Trojan.

7 Q. And how was the Trojan designed so people would
8 click on it?

9 A. It looked like a picture viewer, and it actually
10 contained the pictures of the car that the buyer
11 was interested in, but silently, it could install the
12 virus.

13 Q. So when a person clicked on the picture of the car,
14 the virus would launch?

15 A. No. He would have to run an executable, and then
16 the picture viewer would pop up. You would be able to
17 cycle through pictures, but in the meantime, in the
18 background, Trojan was installed.

19 Q. And what picture of yours did you use?

20 A. It was custom made. It was not — but it looked
21 like a Kodak. It had the icon from Kodak and the
22 name.

23 Q. And did you write that executable, or did
24 Mr. Nicolescu?

25 A. Nicolescu did.

Mr. Tiberiu Danet - Direct

1 Q. Now, once the executable, once the virus was opened,
2 what happened to the victim's computer?

3 A. Nothing besides — it didn't do anything to the
4 computer besides the fact it would allow us to put the
5 fake listing right on eBay's website so to speak.

6 Q. Okay.

7 A. But only on that computer. If they would go to
8 another computer, they would not be able to see the
9 listing we wanted them to see.

10 Q. And what was the benefit of taking over that
11 computer with an eBay option?

12 A. Because before doing that, most of them were saying
13 that they can't find the — that they had received the
14 e-mail that was fake.

15 The second chance offer, that's how it was
16 called, but they can't find anything about it on the eBay
17 website.

18 So after receiving that e-mail, most of the
19 people who were going to the eBay website to find
20 something about that, they were not able to find
21 anything.

22 So by placing an actual listing with a "buy
23 now" button on eBay that actually wasn't on eBay, but
24 they would see it as being on eBay, they were more
25 trustful to use it.

Mr. Tiberiu Danet - Direct

1 Q. And prior to launching the virus, did you understand
2 how it worked? You knew it would take over a computer,
3 correct?

4 MR. GOLDBERG: Objection.

5 THE COURT: Sustained.

6 BY MR. BROWN:

7 Q. Were you, as you are writing code, were you aware of
8 what the code would do?

9 A. I was aware what the code would do, but I was the
10 one that wrote the web interface for the Trojan. So I
11 was not designing it or coding the actual Trojan; I was
12 just — I just coded, for example, pages that had been on
13 the back end on our server that would allow us to see who
14 ran the virus, like from what I see and changing
15 information regarding the vehicle.

16 I could change what the user actually sees,
17 like you could change the car's picture, the car's
18 description on the fly.

19 Q. So your role was sort of to support the virus?

20 A. Yes.

21 MR. GOLDBERG: Objection.

22 THE COURT: Sustained.

23 BY MR. BROWN:

24 Q. What was your role in relation to the virus?

25 A. I was following his specifications. Nicolescu was

Mr. Tiberiu Danet - Direct

1 designing the Trojan, and I was following specifications
2 to create .PHP files in the back end on our server that
3 would sustain this Trojan, that would help it work.

4 Q. Okay. And what is a .PHP file?

5 A. It is a page interpreted by a web server, basically
6 a web page, a dynamic web page.

7 Q. So you were creating web pages that helped the virus
8 run?

9 A. Yes.

10 Q. Did these web pages also help organize data
11 collected by the virus?

12 MR. GOLDBERG: Objection.

13 THE COURT: Sustained.

14 MR. GOLDBERG: May we approach, your Honor?

15 THE COURT: You may.

16 (Side bar held on the record:)

17 MR. GOLDBERG: Thank you, your Honor. We
18 are about 50 minutes into this examination and I have
19 interposed many objections, most based on the leading
20 nature of the questions.

21 And I think what has become obvious is that
22 the Government is leading the witness, and when an
23 objection is sustained, the witness already knows what
24 the Government is getting at.

25 So I am asking the Court to, if the Court

Mr. Tiberiu Danet - Direct

1 would instruct the Government to limit its leading
2 questions, so I don't have to object to every question,
3 and the witness is not, in fact, led?

4 THE COURT: You are, in fact, doing an
5 extraordinary amount of leading, and I am going to
6 instruct you to stop it.

7 MR. BROWN: Yes, ma'am.

8 (Side bar concluded.)

9 BY MR. BROWN:

10 Q. What did your web pages do with the virus?

11 A. They would be able to show the infected computer,
12 they would be able to alter information shown to those
13 infected computers regarding the eBay details, like car
14 picture, car detail, account where the money was supposed
15 to be wired to.

16 Q. How did your web pages support the virus?

17 A. The Trojan accessed those web pages — for example,
18 the Trojan was installed on the computer. Then — and it
19 was giving us the specific ID, every car, like our
20 vehicles had a specific ID.

21 And then, this Trojan had to request
22 information from the server, the central server regarding
23 the — regarding this information. The server would get
24 based on that idea would get information from the
25 database, and it would extract detail from the — like

Mr. Tiberiu Danet - Direct

1 the car description. It would send it back to the
2 infected computer, and the infected computer would save
3 it to the hard disk and display. So everything — the
4 Trojan would get everything from the server or most
5 everything.

6 Q. And who created the auction ID?

7 MR. GOLDBERG: Objection.

8 THE COURT: Sustained.

9 BY MR. BROWN:

10 Q. Where did the auction IDs come from?

11 A. They were just named data that we made up, and
12 everybody make up — for example, if somebody — if I
13 would post an auction, I make up an ID with a prefix of
14 pay M1, and everybody create an ID with their prefix,
15 like with their alias prefix of whatever.

16 Q. And how did your websites help the auction process
17 operate?

18 A. Are you referring to these web pages?

19 Q. No, no. As the web pages were working, what was the
20 result in the fraud, in the eBay fraud?

21 MR. GOLDBERG: Objection.

22 THE COURT: Overruled.

23 A. Well, these were — you needed to support the
24 Trojan. The Trojan has no meaning if it can't get data
25 from somewhere. But again, I was not the one — I

Mr. Tiberiu Danet - Direct

1 created some of those web pages, not all of them.

2 Q. How many people were creating web pages?

3 A. At that point at the beginning or after that?

4 Q. At the beginning.

5 A. Just me and Nicolescu.

6 Q. Did there come a time when there were other
7 people?

8 A. Yeah, later.

9 Q. How much later?

10 A. Probably 2012 or maybe '11.

11 Q. And do you know why other people joined?

12 A. Nah. I was not given that information. It was
13 Nicolesu's decision to get people to join.

14 MR. GOLDBERG: Objection.

15 THE COURT: Overruled.

16 BY MR. BROWN:

17 Q. And did you talk to those people as well?

18 A. No. I never knew. I chatted with one of them.

19 Q. Who?

20 A. His nickname was Linx, I think it was — he was
21 pretty good at programming. I didn't know him at
22 all.

23 Q. And how long did you participate in this fraud
24 scheme?

25 A. From 2007 to 2016, but it was something that

Mr. Tiberiu Danet - Direct

1 went —

2 MR. GOLDBERG: Objection.

3 THE COURT: Sustained.

4 BY MR. BROWN:

5 Q. And let's jump ahead to 2016.

6 September 20th, 2016, what happened that
7 day?

8 A. I was arrested that day.

9 Q. And do you know why you were arrested?

10 A. For participating in this scheme.

11 Q. And as a result of your arrest, were you extradited
12 to the United States?

13 A. Yes, ten and a half months later.

14 Q. And in fact, also, as a result of that arrest, your
15 apartment was searched, correct?

16 A. Yes.

17 Q. And were you present for your extradition
18 proceeding?

19 A. I was held in jail in Romania, and yeah, there were
20 a few court hearings regarding the extradition.

21 Q. And the result was you were extradited to America?

22 A. Yes.

23 Q. Now, when you came to America, did you have an
24 attorney represent you?

25 A. Yes.

Mr. Tiberiu Danet - Direct

1 Q. Did you talk to your attorney?

2 A. Yes, frequently.

3 Q. And did you talk to him about the case?

4 A. Of course.

5 Q. Did you talk to him about the evidence?

6 A. Yes.

7 Q. Did you talk to him about strategies without
8 detailing what those strategies were?

9 A. Yes.

10 Q. Did there come a time when you entered a plea of
11 guilty in this case?

12 A. Yes.

13 Q. And was it a plea of guilty in open Court or subject
14 to a plea agreement?

15 A. It was subject to a plea agreement.

16 Q. Okay. And was that plea agreement with the
17 United States of America, Northern District of Ohio?

18 A. Yes.

19 Q. And in fact, was that plea agreement signed by
20 you?

21 A. Yes, I signed.

22 Q. Signed by your attorney?

23 A. Yes.

24 Q. Signed by me?

25 A. Yes.

Mr. Tiberiu Danet - Direct

1 Q. What do you understand that plea agreement to
2 be?

3 A. Regarding the time or charges or account or —

4 Q. We will get to all of it, but let's start with
5 time. What do you understand the plea agreement to be
6 for time?

7 A. So the plea agreement is for nine to 12 years.

8 Q. Nine to 12 years?

9 A. Yeah.

10 Q. And who do you understand that that decision to rest
11 with, what that sentence will be?

12 A. Solely with the Judge.

13 Q. Do you understand that to rest with me?

14 A. No.

15 Q. Only with the Judge?

16 A. Yes.

17 Q. What do you understand the maximum amount of time
18 you could have gotten was?

19 A. Well, that was pretty vague, but I was advised by my
20 attorneys to take this, so it was more than 12 years.

21 Q. Do you know how much more?

22 A. Not exactly.

23 Q. Okay. Were you made any additional promises other
24 than your sentence would be between nine and 12 years?

25 A. No.

Mr. Tiberiu Danet - Direct

1 Q. Were you made any other — any guarantees of
2 anything?

3 A. No.

4 Q. How many times have we met?

5 A. Five, six times.

6 Q. And during those times, were you given any
7 benefits?

8 A. Such as what? No.

9 Q. Well, you were purchased lunch, correct?

10 A. Yes. I was purchased lunch.

11 Q. Did we meet in jail or elsewhere?

12 A. Elsewhere.

13 Q. Did we meet in an FBI office?

14 A. Yes.

15 Q. Were you in custody at the time?

16 A. Yes.

17 Q. You were not allowed to walk around the
18 neighborhood?

19 A. If I was what?

20 Q. Were you allowed to leave the office, the FBI
21 office?

22 A. No.

23 Q. Were you allowed to leave the presence of an FBI
24 agent?

25 A. No.

Mr. Tiberiu Danet - Direct

1 Q. Was that a benefit to you, to be taken out of jail
2 to an FBI office?

3 A. No, quite the opposite.

4 Q. Okay. Was the lunch that you were provided a
5 benefit?

6 A. I had to have one for the day, so I don't consider
7 it a benefit.

8 Q. Were you made any promises about anybody in
9 Romania?

10 A. No.

11 Q. Were you made any promises about what might happen
12 to you when you return to Romania?

13 A. No.

14 Q. Were you — what do you understand your
15 responsibility under the plea agreement to be?

16 A. My responsibility, I just pled guilty to the counts
17 I was guilty of.

18 Q. Were you expected to do anything else under the
19 terms of the plea agreement?

20 MR. GOLDBERG: Objection.

21 THE COURT: Overruled.

22 A. Yeah. I was expected to cooperate.

23 Q. What do you understand cooperation to be?

24 A. Everything, including this testimony where I am
25 supposed to tell the truth.

Mr. Tiberiu Danet - Direct

1 Q. Were you asked to provide information prior to
2 today?

3 A. Yes.

4 Q. Information about the case?

5 A. Yes.

6 Q. Information about your knowledge of the case?

7 A. Yes.

8 Q. Were you asked to identify people involved in the
9 case?

10 A. Yes.

11 Q. Did those people include members of your family?

12 A. Yes.

13 Q. Did you provide that information?

14 A. Yes, I did.

15 Q. Were you asked to provide passwords to accounts?

16 A. Yeah.

17 Q. Did you provide that information?

18 A. Yes, to the best of my knowledge.

19 Q. Do you know if all of the passwords you provided
20 worked?

21 A. As far as I know, no, not all of them did.

22 Q. Did you provide additional information about the
23 passwords that didn't work?

24 A. Yes. I was given a laptop where I worked inside the
25 jail trying to see what went wrong.

Mr. Tiberiu Danet - Direct

1 Q. When you say you were given a laptop, was it
2 accessible to the internet?

3 A. No.

4 Q. Was it working?

5 A. Yes. It was working.

6 Q. But it couldn't connect to the internet?

7 A. No, it couldn't.

8 Q. Did it have programs loaded on it?

9 A. No. It just had a virtual machine with my system on
10 it, my — a copy of my system, so I would be able to
11 access.

12 Q. Did you have to give it back to the FBI?

13 A. I think it is still in the jail right now.

14 Q. Did you have to give it to somebody in the jail?

15 A. It sits in an area, it is called a video
16 conferencing area. One is constantly there, and I would
17 go except for the weekends, and I would go there
18 sometimes during the week for just an hour or two or
19 during the week, four hours.

20 Q. So it was under supervision?

21 A. Yes, except for the weekend.

22 Q. Were you allowed to take the computer out of this
23 room?

24 A. No.

25 Q. Now, also, were you required to provide the

Mr. Tiberiu Danet - Direct

1 monikers, the nicknames of everybody in the
2 group?

3 A. Yes.

4 Q. Including your family members' monikers?

5 A. Yes.

6 Q. And were any promises made about any of the other
7 people you provided information about?

8 A. None.

9 Q. Were you provided with a statement of facts as part
10 of this plea agreement?

11 A. Yes.

12 Q. Did you have a chance to review those statement of
13 facts?

14 A. Yes. I actually made a few statements I didn't
15 agree with.

16 Q. Were you able to discuss with your attorney
17 statement of facts?

18 A. Yes.

19 Q. And as part of the plea agreement, did you agree
20 with the statement of facts as they were presented to you
21 on the day of the plea?

22 A. Yes.

23 Q. As part of the plea agreement, did you talk about
24 virtual private networks?

25 MR. GOLDBERG: Objection.

Mr. Tiberiu Danet - Direct

1 THE COURT: Overruled. Answer that yes or
2 no, sir, if you remember.

3 THE WITNESS: Yes.

4 BY MR. BROWN:

5 Q. Did you admit to knowing what a virtual private
6 network is?

7 MR. GOLDBERG: Objection.

8 THE COURT: Overruled. You may answer that
9 yes or no.

10 THE WITNESS: Yes.

11 BY MR. BROWN:

12 Q. As part of the eBay fraud that you were engaged in,
13 did you use virtual private networks?

14 A. Yes.

15 Q. How did you use virtual private networks.

16 A. Virtual private network would allow me and the
17 others to stay anonymous.

18 Q. How?

19 A. That's basically what a virtual private network
20 does. You have — you buy an account with like private
21 internet access, and by logging in, you have a different
22 IP that couldn't be traced back to you when using the
23 internet.

24 Q. And when you say you and the others, were those
25 others members engaged in the same fraud you were engaged

Mr. Tiberiu Danet - Direct

1 in?

2 A. Yes.

3 Q. And were they — were you using virtual private
4 networks — how long were you using these virtual private
5 networks during the fraud scheme?

6 A. All the time among other things.

7 Q. Okay. Starting in 2007?

8 A. Yes, 2007.

9 Q. Up until the time of your arrest?

10 A. Yes.

11 Q. Was that the sole way you would communicate with
12 members of the fraud scheme?

13 A. You mean through virtual private network?

14 Q. Yes.

15 A. No, but it was just — the only way at the beginning
16 where we would communicate about the scheme.

17 Q. Why?

18 A. So that it couldn't be traced back to us.

19 Q. And what sort of ways would you hide your identity
20 when you were using a VPN?

21 A. Well, there are multiple steps besides using that
22 VPN for obscuring our actual location and IP address that
23 identifies the location.

24 Q. And what are those steps?

25 A. It began from something simple going to something

Mr. Tiberiu Danet - Direct

1 more complex towards the end.

2 Q. Okay. What was the simple beginning?

3 A. The simple beginning was using the Tour network. It
4 is a public service that allows you to do the same thing.
5 This was the first step, and the second step was using
6 AOL's Compuserve, a type of virtual private network.

7 Q. Okay. And on the AOL Compuserve, did you have a
8 name you used?

9 A. Yes. But I can't remember it. This was only used
10 in 2007.

11 Q. Okay. And then, you moved on to another means?

12 A. Yes.

13 Q. AOL Compuserve, or did you still use the Tour
14 network?

15 A. Would still use the Tour, yes, but there were a lot
16 more other steps.

17 Q. And what were those steps after 2007?

18 A. It changed during time. I can't remember every
19 precise way to connect to the internet during each year,
20 but I know what it ended up being.

21 Q. What did it end up being?

22 A. Some of the members of the conspiracy would have
23 antennas that would connect with Wi-Fi networks belonging
24 to, say, neighbors. So you would connect through that.
25 That was the first step.

Mr. Tiberiu Danet - Direct

1 The second step was further connecting from
2 multiple — actually two other servers.

3 Q. Are those the VPN servers you were talking about?

4 A. No. Actually, I am wrong. No. There were these
5 two other servers, were actually computers and technical
6 computers?

7 But before that, after connecting to the
8 Wi-Fi, we would connect to Tour and then to these two
9 other computers that belonged — that were actually
10 infected computers, then a VPN, and there were like five
11 steps.

12 Q. Okay. And when you say infected computer, do you
13 mean a computer infected with the virus?

14 A. Yes, with the virus.

15 Q. With the virus Mr. Nicolescu designed to
16 do —

17 MR. GOLDBERG: Objection.

18 THE COURT: Sustained.

19 BY MR. BROWN:

20 Q. Was that the same virus that you knew about in
21 2007?

22 MR. GOLDBERG: Objection.

23 THE COURT: Overruled.

24 A. Yes. It was the same virus, but it got different
25 functionality towards the end. This functionality of

Mr. Tiberiu Danet - Direct

1 connecting through it was not available in 2007.

2 Q. Who added that functionality?

3 A. Nicolescu did.

4 Q. Did you work on that functionality?

5 A. No.

6 Q. Again, what is the Tour network?

7 A. It is a network of thousands of computers, computers
8 that allows you just like a VPN to stay anonymous.
9 Basically, instead of making a connection from your house
10 to the internet, it goes through like a couple of
11 computers until it connects itself. And wherever you
12 connect it, it can face it back because it goes through
13 different nodes.

14 Q. Does it change the appearance of your IP address?
15 Is that what you mean?

16 A. Yeah.

17 Q. So is it fair to say you log on to the Tour network
18 with IP address 1, 2, 3, 4, and you leave the Tour
19 network with IP address 5, 6, 7, 8?

20 A. Yes. It is usually with the Tour network. If you
21 don't set it up at all, it is used as a different address
22 all the time.

23 MR. BROWN: Can we pull up 1874 at this
24 time?

25

Mr. Tiberiu Danet - Direct

1 BY MR. BROWN:

2 Q. Okay. So here is — could you describe what we are
3 looking at here?

4 A. Yes. That's exactly right. From our computers, we
5 connect to Wi-Fi network or open Wi-Fi network that
6 doesn't have an encryption key.

7 Q. And at that step, is that the laptop of the house?

8 A. Yes. It doesn't have to be a laptop.

9 Q. Was that normally your house or somebody else's
10 house?

11 A. Everybody followed the same steps that is connected
12 to the internet.

13 Q. Okay. So then, after the step at the house, then
14 what happened?

15 A. Connecting to the Wi-Fi network. Actually, first
16 you would connect to, say — it would say one week this
17 antenna right here. That belonged to me or Nicolescu or
18 somebody else was using for a week?

19 And then we would connect to that person's
20 house; then through his house to that antenna, then to
21 the Tour network that same infected computer and VPN, so
22 it was basically pretty much untraceable. And at the end
23 of the week, we change the antenna of the connection so
24 it wouldn't be used too much.

25 Q. Where are you getting the antenna?

Mr. Tiberiu Danet - Direct

1 A. They are bought.

2 Q. By the people you were working with?

3 A. Actually, I think they were bought by Nicolescu who
4 had given all the members —

5 MR. GOLDBERG: Objection.

6 THE COURT: Sustained.

7 BY MR. BROWN:

8 Q. Now, once you were on, let's say, the server at the
9 top of the left, what would you do when you would VPN
10 into a server?

11 A. All the connections that you would make after this
12 VPN, you had the IT from the VPN, so it was untraceable.
13 Even if this was identified, the IP of the VPN, it
14 couldn't go back so many steps to go back to you.

15 Q. So let's look at some of these logo.

16 EBay, what is the benefit of having an
17 anonymous address on eBay for your scheme?

18 A. Besides not using your own, so that you can be
19 identified. You could connect, you could have an IP that
20 belonged to a certain American state. Say, if you create
21 an account in California, you usually need an IP address
22 that would belong to California.

23 Q. And why would you want your IP address to match your
24 listing?

25 A. So that everything would look correct. Usually when

Mr. Tiberiu Danet - Direct

1 it is somebody from California, they would have a
2 California IP.

3 Q. And how about with the gmail address or the gmail
4 icon? What's the benefit of using an anonymous VPN to go
5 on to gmail?

6 A. Well, again, for not using your own IP, give you a
7 chance to use a different IP every time. But actually,
8 after the VPN, you could connect to every website on the
9 internet using that IP.

10 It was not just gmail or Facebook or all the
11 items that are presented here. And most of the times
12 before accessing such a website, again, you choose a
13 server, a process server, something that allows you to
14 connect to those websites that would belong to the
15 location that you needed it to belong to; be it Facebook
16 or gmail or Craigslist. If I wanted a server from
17 Georgia, I would be able to get an IP from Georgia.

18 Q. Now, what is the call fire icon that you see here?
19 Does that mean anything to you?

20 A. It is an online faxing service. It will be able to
21 receive faxes.

22 Q. And was that, in fact, used by you or the other
23 members when you were doing fraud?

24 A. Yes.

25 Q. Why?

Mr. Tiberiu Danet - Direct

1 A. The buyers wouldn't — would be requested to send a
2 fax with the receipt from their bank, with the actual
3 wire transfer details so that we could verify.

4 Q. So you could get a fax number?

5 A. Yes. You can get a fax number that you can check
6 online.

7 Q. And it would not come back to Romania, the number
8 wouldn't. It would be a U.S. looking number?

9 A. Yes, it is a U.S. looking number.

10 Q. But you would be able to get whatever syntax?

11 A. Yes. You log in on cold fire and see the images.

12 Q. And what about Craigslist? What did the group use
13 the VPN to log on anonymously under Craigslist?

14 A. For a short while Craigslist was used to list
15 vehicles just like on eBay with the purpose of getting
16 interested buyers e-mail.

17 Q. Was it used for anything else?

18 A. I think at one point it was used for —

19 MR. GOLDBERG: Objection.

20 THE COURT: Sustained.

21 BY MR. BROWN:

22 Q. And what is, if you know, GMX?

23 A. It is an e-mail service.

24 Q. And what was the benefit for the group of using the
25 VPN to log on to GMX anonymously?

Mr. Tiberiu Danet - Direct

1 A. Well, again, collectively, for all these services,
2 it was to stay anonymous. That was the bottom line.

3 Q. Could you repeat that?

4 A. So for all these services listed, the bottom end for
5 everything else, the benefit of using the VPN and all the
6 chain of connections above was to stay anonymous.

7 Q. Okay.

8 MR. BROWN: Can I approach the Defendant or
9 the witness?

10 THE COURT: Yes.

11 BY MR. BROWN:

12 Q. Would you please take a look at Exhibit 1415?

13 A. Yes.

14 Q. Do you recognize what that is?

15 A. Yes. It is —

16 Q. I'm sorry. Can you explain what that is?

17 A. It is a Wi-Fi antenna. It is just like this one but
18 much more powerful.

19 Q. Okay. And is that the same sort of Wi-Fi antenna
20 you used in the first step —

21 A. Yes.

22 Q. — that you just described?

23 A. Yes.

24 Q. And could you explain to the jury how you would do
25 it?

Mr. Tiberiu Danet - Direct

1 A. Um —

2 Q. How would you physically set it up?

3 A. You would have to try a lot, and sometimes with a
4 poor connection you would have trouble connecting to some
5 of the Wi-Fi networks.

6 You have to tilt it or put it in a stable
7 place in a position until it worked.

8 Q. So let's take a step back. What is the part you are
9 holding in your right hand right now?

10 A. This is the antenna.

11 Q. That's a big orange square.

12 A. Yes.

13 Q. And where would you point an antenna if you were in
14 your apartment?

15 A. Say I had an apartment building, that way I could
16 try pointing it like this or rotating like this or
17 tilting it like this until I get the best signal.

18 Q. And what's the purpose of that big orange
19 square?

20 A. It has good reception compared to the little
21 thing.

22 Q. And the little thing you are pointing to, can you
23 describe this?

24 A. This is probably the router, the antenna, they're
25 called antenna.

Mr. Tiberiu Danet - Direct

1 Q. So it is a two-piece device. It has got two
2 antennas, one is a big orange square and the other —

3 A. There are three antennas.

4 Q. Three antennas?

5 A. This is the fold one that it comes with. It comes
6 with three antennas like this. This is the — the more
7 powerful antenna.

8 Q. And what does the antenna pull in?

9 A. The signal from the Wi-Fi.

10 Q. Just like a TV antenna but for Wi-Fi?

11 A. Yeah. It is like any antenna.

12 Q. And what is the white box with all the antennas?

13 A. This is the router, what you have in your house, and
14 all the internet connections go through it.

15 Q. And once you find a Wi-Fi signal using one or all
16 three of those antennas, what's the next step you take?

17 A. Depending on the Wi-Fi network, you maybe have to
18 break the encryption if you could.

19 Q. Okay. So it might be encrypted. That's where you
20 have to type in a password?

21 A. Yes.

22 Q. And how would you do that? How do you break
23 encryption?

24 MR. GOLDBERG: Objection.

25 THE COURT: Overruled.

Mr. Tiberiu Danet - Direct

1 BY MR. BROWN:

2 Q. You specifically.

3 A. There is two or usually two types of protocols used
4 for encrypting, and one of them is prone to be incorrect.
5 So one of them is very poor, and some people still use
6 that. Actually, the router comes defaulted with that
7 setting on to delete the protocol. So that is cracked
8 easily if you get a good signal to the Wi-Fi spot.

9 Q. And if it doesn't have encryption?

10 A. Then, it is only to put in any password, and you
11 just connect to the Wi-Fi network just like in a public
12 place.

13 Q. Okay. Now, how did you send e-mails to members of
14 the group? Like —

15 A. Regarding — whenever I was communicating about the
16 scheme, I would go through all of this chain to connect
17 to the internet, and then I will send my e-mail.

18 Q. And did you have an e-mail address you used when you
19 were talking about the criminal online eBay auction
20 scheme?

21 A. Yes.

22 Q. What was your e-mail?

23 A. The last one I had was amightysa@gmail.com.

24 Q. And what did sa in amightysa stand for?

25 A. Really nothing. It was just amighty wasn't

Mr. Tiberiu Danet - Direct

1 available, so I just typed two more letters.

2 Q. Okay. And that was a gmail?

3 A. Yes. Previously, I think I had the same handle at
4 GMX.

5 Q. Okay. And by "handle" you mean e-mail names?

6 A. Yes, what comes before that.

7 MR. BROWN: Your Honor, may I approach the
8 witness to take that back?

9 THE COURT: You may.

10 BY MR. BROWN:

11 Q. And by the time you were using amightysa@gmail.com,
12 about how many were you communicating with concerning the
13 criminal scheme?

14 A. Personally about four.

15 Q. Okay. And which e-mail addresses were you
16 communicating with?

17 A. Most commonly Master Fraud at GMX.com, and then the
18 Minolta 9797. I forget the domain, if it was aol.com or
19 not.

20 Q. Who were the other two?

21 A. My brother.

22 Q. What was his e-mail address?

23 A. The handle was — he changed it at least once. One
24 of the handles was r-a-d-o-b-d-s.

25 Q. And what were the other ones he used?

Mr. Tiberiu Danet - Direct

1 A. Rasputin.

2 Q. And how was Rasputin spelled?

3 A. R-a-s-p-u-t-i-n.

4 Q. Were any numbers used in it?

5 A. I can't recall.

6 Q. And who was the fourth person?

7 A. I communicated with Linx.

8 Q. Linx?

9 A. Linx is the — his real name is Catalin Dima,
10 another person that did some coding, some or beginning in
11 2012, I think, for a couple of years.

12 Q. And your brother's name is what?

13 A. Valentin.

14 Q. Also Danet?

15 A. Yes.

16 Q. And when you communicated with him, you used
17 amightysa?

18 A. Yes.

19 Q. Did you ever use a personal more identifiable e-mail
20 name?

21 A. Yes, but not for communicating anything regarding
22 this.

23 Q. Okay. And was that the same with them, did you ever
24 send criminal e-mails to any other handle?

25 MR. GOLDBERG: Objection.

Mr. Tiberiu Danet - Direct

1 THE COURT: Sustained.

2 BY MR. BROWN:

3 Q. When you would communicate with them about criminal
4 matters, would you always end in the process you just
5 described?

6 MR. GOLDBERG: Objection.

7 THE COURT: Sustained.

8 Q. How would you send an e-mail to one of those four
9 e-mail addresses concerning criminal activity?

10 MR. O'SHEA: Objection.

11 Q. Could you describe the steps?

12 THE COURT: Sustained.

13 BY MR. BROWN:

14 Q. Other than e-mail, did you communicate about
15 criminal activities with those four individuals?

16 MR. O'SHEA: Objection.

17 THE COURT: Side bar.

18 (Side bar held on the record.)

19 MR. O'SHEA: Look, I know there is a
20 conspiracy count, but the questions are way too vague and
21 leading.

22 THE COURT: The problem I am having with the
23 questions is the broad term "criminal activity."

24 MR. BROWN: I can take that out and just ask
25 how you communicate with the four.

Mr. Tiberiu Danet - Direct

1 THE COURT: The reason I sustained the
2 objections is because of the broadness of it without any
3 specificity.

4 MR. BROWN: Thank you, your Honor.

5 (Side bar concluded.)

6 BY MR. BROWN:

7 Q. How else would you communicate with those four
8 individuals?

9 A. Regarding the criminal scheme or just personally?

10 Q. Let's start with personally.

11 A. Personally, through phone, through a chip server,
12 where we had different handles, and we would connect
13 normally. So that is like from your phone, from your
14 computer, from your own IP.

15 Q. Okay. And what were those personal handles that you
16 had for, first, let's start with Master Fraud?

17 A. So Nicolescu had on this chat server that was
18 actually installed in my house, he had the user name
19 obe.

20 Q. And how about Minolta 9797?

21 A. Nicolescu had the handle for —

22 MR. GOLDBERG: Objection.

23 THE COURT: Overruled.

24 A. F-e-r-d-y. Everybody had a different handle from
25 the mobile to connect to. The mobile had one handle.

Mr. Tiberiu Danet - Direct

1 The computer or laptop that was connected had a different
2 handle.

3 Q. How about your brother?

4 A. He had Balint, B-a-l-i-n-t.

5 Q. Okay. And how about Catalin Dima?

6 A. I don't know. I didn't communicate with him
7 personally.

8 Q. And what was your handle, your personal handle?

9 A. Romeo.

10 Q. Now, you said you would use telephones. Again, this
11 is personal telephones?

12 A. Yes.

13 Q. And you said a chat server?

14 A. Yes.

15 Q. What chat server?

16 A. Jabber chat server.

17 Q. Jabber.

18 A. Yeah. That's a — yeah, that's a protocol.

19 Q. And what is a Jabber chat server?

20 A. It is a chat server that there is a few, I mean,
21 more than a few public Jabber servers that you can use
22 for free, but you can also install your own if you want
23 to service them.

24 Q. Okay. And how do you communicate over a
25 chat server? What does that communication look

Mr. Tiberiu Danet - Direct

1 like?

2 A. Just like any other chat communication on Facebook
3 or laptop.

4 Q. Like text message?

5 A. Yes. Short text messages.

6 Q. Okay. And was this Jabber server open to the
7 public, or did you have to log in?

8 A. Yes. It was open to the public.

9 Q. But the one in your house?

10 A. Yes.

11 Q. So anybody could access the one in your house?

12 A. Yes.

13 Q. You said you also had names for — or I'm sorry.

14 That's the way you communicated for
15 personal, and you said there was a way you communicated
16 for criminal conversations?

17 A. Yes.

18 Q. And what were those methods?

19 A. Well, whenever I would discuss anything related
20 to this criminal scheme, I would always go through
21 this chain in connecting like that every time and then
22 e-mail.

23 Q. Was it always e-mail?

24 A. No. Could be another chat server, but it had
25 different handles. It was not a personal one, just

Mr. Tiberiu Danet - Direct

1 another one.

2 Q. Okay. And what chat server was that?

3 A. It changed during the time.

4 Q. Okay. And in 2016, what chat server were you using
5 for criminal communications?

6 MR. O'SHEA: Objection.

7 THE COURT: Overruled. Based upon his prior
8 answer, I am going to allow it.

9 THE WITNESS: I don't recall. It was
10 different servers, but I can't recall the name or the
11 domain because it changed.

12 BY MR. BROWN:

13 Q. Do you recall the program that you used?

14 A. Yeah. For windows Pidgin.

15 Q. Pidgin?

16 A. Yeah.

17 Q. And was that open to the public?

18 A. Yes, it was public available software.

19 Q. So anybody could log on to Pidgin and see your
20 communications?

21 A. No. You would have your own user name and
22 password. Anybody could use Pidgin as a software. We
23 had our own account.

24 Q. But could users of Pidgin see your communications to
25 other members just out in the open?

Mr. Tiberiu Danet - Direct

1 A. No.

2 Q. How did you prevent that from happening?

3 A. You don't have to prevent it; just like logging in
4 with your password, you have your own account. These
5 communications were encrypted, too.

6 Q. Okay. So you had to have — you only communicated
7 with people in your account?

8 A. Yes, only with people in your account.

9 Q. A contact list?

10 A. Yes.

11 Q. And you also said they were also encrypted?

12 A. Yes.

13 Q. What encryption program did you use.

14 A. It is called OTR, off the record.

15 Q. And what was your user name for Pidgin OTR?

16 A. On my personal or my — because I was using Pidgin
17 with my personal server, with handle Romeo, but I was
18 using the same setup on the account that I was using for
19 criminal.

20 Q. Okay. How about criminal since we established
21 criminal?

22 MR. GOLDBERG: Objection.

23 THE COURT: Overruled.

24 THE WITNESS: It was the same for me
25 amightysa.

Mr. Tiberiu Danet - Direct

1 BY MR. BROWN:

2 Q. And what handles did you communicate with on the
3 criminal Pidgin?

4 MR. O'SHEA: Objection.

5 THE COURT: Again, based upon his answer
6 several answers ago, I am going to overrule the
7 objection.

8 A. One of the — again, these user names change so
9 often that I don't remember all of them, but for example,
10 Nicolescu because I was communicating with him through
11 the server.

12 MR. GOLDBERG: Objection.

13 THE COURT: Overruled.

14 A. Had at one time Master Fraud, the same as the
15 e-mail, but at another point change to something Q W W X
16 or something like that, and Miclaus had —

17 MR. O'SHEA: Objection.

18 THE COURT: Overruled.

19 THE WITNESS: Minolta, the same — Minolta
20 9797 had the same as his e-mail. I know there was my
21 brother was using a variation of Rasputin, but it had
22 some dollars in it. It is hard to remember all the
23 numbers and dollars in the user name.

24 BY MR. BROWN:

25 Q. Now, were you able — withdraw that.

Mr. Tiberiu Danet - Direct

1 MR. BROWN: Your Honor, I'm sorry. I am
2 just trying to figure out the order of my questions with
3 the afternoon break coming up, and I didn't want to jump
4 into it.

5 THE COURT: Are you asking that —

6 MR. BROWN: No, no.

7 THE COURT: — to break at this point
8 because I am happy to.

9 MR. BROWN: Unless you would like to, your
10 Honor. It is 2:30.

11 THE COURT: I think it is closer to 2:40,
12 and I am planning on 2:45. So we will take a break now.
13 Folks, remember the admonition. All rise for the jury.

14 (Recess had.)

15 THE COURT: Please be seated. Mr. Brown,
16 you may continue.

17 MR. BROWN: Thank you, your Honor.

18 BY MR. BROWN:

19 Q. Now, before the break, we were talking about a
20 Jabber server in your house.

21 Do you recall that?

22 A. Yes.

23 Q. And you said it was open to the public?

24 A. Yes.

25 Q. Could anybody log on to your Jabber server?

Mr. Tiberiu Danet - Direct

1 A. If you knew the address, the domain name, yes.

2 I mean, you would create an account first and then log
3 in.

4 Q. So not everybody could log in?

5 MR. O'SHEA: Objection to the form of the
6 question.

7 THE COURT: Sustained.

8 BY MR. BROWN:

9 Q. It was password protected?

10 A. You needed to create an account, which you could
11 do.

12 Q. And with whom would you have to create an account?

13 A. By knowing the address of the server, you would just
14 put it in Pidgin and hit the create account button, and
15 you could create an account.

16 Q. So is it fair to say because it was in your
17 apartment you controlled the server, correct?

18 MR. O'SHEA: Objection to the form of the
19 question.

20 THE COURT: Sustained.

21 BY MR. BROWN:

22 Q. Did you control the server?

23 A. What do you mean by "control"?

24 Q. Could you control who knew the address?

25 A. The address, if anybody wanted to register, they

Mr. Tiberiu Danet - Direct

1 could register, but it would be hard to know the address
2 if somebody didn't tell you.

3 Q. So it was not an obvious address?

4 A. Yes.

5 Q. And how about the criminal Jabber server, was that
6 open?

7 MR. GOLDBERG: Objection.

8 THE COURT: Overruled.

9 A. No. I don't think it was. It was changed several
10 times, so it was not one server during the whole period.
11 Sometimes it was changed monthly.

12 Q. And what was the purpose of changing it monthly?

13 A. One of the reasons was that the server on which it
14 was installed would be disconnected by whoever sold it
15 because the credit card information or —

16 Q. Whose credit card did you use to register it?

17 A. Credit cards obtained through websites like the one
18 I discussed about or through other means by using the
19 Trojan.

20 Q. So stolen credit cards?

21 A. Yes.

22 Q. And about — when were you using the Jabber server,
23 about what time period?

24 A. The criminal, for the criminal?

25 Q. Yeah, criminal.

Mr. Tiberiu Danet - Direct

1 A. At least four or five years prior to my arrest.

2 Q. So somewhere between 2011 to 2016?

3 MR. GOLDBERG: Objection.

4 THE COURT: Sustained.

5 BY MR. BROWN:

6 Q. So for that — so you were getting at that time
7 credit cards from the Bayrob Trojan?

8 MR. GOLDBERG: Objection.

9 THE COURT: Sustained. Watch the leading.

10 MR. BROWN: I'm sorry, your Honor.

11 BY MR. BROWN:

12 Q. How could you get credit cards from the Bayrob
13 Trojan?

14 A. There were several methods. For example, one of
15 them, when users or the infected computers would visit
16 popular websites such as Facebook or instead of, let's
17 say, Facebook — there were others, too — they would get
18 a page that was not authentic, that required them to
19 verify their account by putting in their credit card
20 information.

21 Q. And how did the Trojan use that page? How did it
22 present that page to somebody?

23 A. Based on Nicolesu's input. If that computer was
24 selected to be shown such a page, it would be shown that
25 page once when visiting Facebook.com, and if the user

Mr. Tiberiu Danet - Direct

1 would input their credit card information and click next,
2 it would just say "okay. Your account was verified."

3 It would, of course, save the credit card,
4 and then next time the user accesses the same website, it
5 would go to the default, the actual Facebook.com.

6 Q. And did that kind of page appear only on an infected
7 computer?

8 MR. GOLDBERG: Objection.

9 THE COURT: Overruled. You may answer.

10 A. Yes, only on the infected computer.

11 Q. So the Trojan could collect that kind of credit card
12 information on infected computers?

13 MR. GOLDBERG: Objection.

14 THE COURT: Sustained.

15 BY MR. BROWN:

16 Q. What happened to the credit card information after
17 it was pulled off of your Facebook, for example? Where
18 would it go?

19 A. It would be saved in a file, and it would be used
20 either for buying domain names or servers maybe for the
21 infrastructure or, for example, the faxing service
22 account, anything that required a pay.

23 Q. Where was this file?

24 A. Excuse me?

25 Q. Where was the file? You said it was saved in a

Mr. Tiberiu Danet - Direct

1 file.

2 A. It was saved on the central server and then
3 downloaded from there.

4 Q. Okay. What do you mean by "central server"?

5 A. There was a server that would — we would use
6 to monitor the Trojan, such as computers, the list
7 of computers, and then activity relating to the
8 Trojan.

9 Q. Okay. And could I show you 1873, which has already
10 been shown to the jury? Okay.

11 Do you recognize this diagram? Do you
12 recognize what's being displayed in this diagram?

13 A. Yes.

14 Q. Okay. What is the top line in this exhibit?

15 A. Such a server I mentioned, command and control
16 server.

17 Q. So top line is central server. And what is this
18 relationship to the next two lines?

19 A. Well, to be honest, I don't know exactly what the
20 second line is. There were servers bought with the
21 OS Omnis and Blue Host.

22 Q. What would you call those servers?

23 A. They were used for different things like later
24 cryptomining tools. Even the Jabber server was installed
25 on something else and the central server.

Mr. Tiberiu Danet - Direct

1 Q. Okay. Would those — what's marked as relay
2 servers, would those servers communicate with the central
3 command and server?

4 MR. GOLDBERG: Objection.

5 THE COURT: Sustained.

6 MR. GOLDBERG: I object to the use — it is
7 leading. He is having it up —

8 THE COURT: No. I will allow it to be used,
9 but please watch the leading.

10 MR. BROWN: Yes, your Honor.

11 BY MR. BROWN:

12 Q. What is the bottom row?

13 A. Just infected computers so I guess.

14 Q. What information would you have on the central
15 server?

16 A. I personally or —

17 Q. Let's start with you personally.

18 A. All the .PHP files I mentioned at the beginning that
19 support Trojan, they were installed on the C & C server.
20 Everything that allowed us — like tables that allowed us
21 to see the infected computers and all the actions you
22 could take for every computer, like say have it show that
23 Facebook page. That's one action, have that specific
24 computer.

25 That's all on the central server along with

Mr. Tiberiu Danet - Direct

1 a lot of other things like the escrow website, a copy of
2 it was there, too. There is just a lot.

3 Q. And when you say a central server would see the
4 infected computer, what do you mean by that?

5 A. There was a list every infected computer would, say,
6 ping another server, and it would show up, it would
7 update like every, say, ten minutes. It has been changed
8 up. Every ten minutes it would send a signal it was
9 online and see whenever a computer was online or not.
10 There were different colors like red for online and red
11 for offline; green for online, that sort of thing.

12 Q. And what do you mean my an infected computer would
13 ping?

14 A. It would just send a signal to this server saying "I
15 am online, I am connected to the internet."

16 Q. So there was a program on the central server that
17 pinged infected computers?

18 MR. GOLDBERG: Objection.

19 THE COURT: Sustained.

20 BY MR. BROWN:

21 Q. How would the central server ping as you described
22 it the infected computer?

23 A. The infected computer would ping the server, and
24 from the server, there was a .PHP page that allowed to
25 see all these computer.

Mr. Tiberiu Danet - Direct

1 Q. And again, what is a .PHP page?

2 A. It was called the ping dash view.PHP.

3 Q. And who created the ping page?

4 A. I did.

5 Q. I would like to pull up Exhibit 1446, page 2. This
6 is Exhibit 1446, page 2.

7 Do you recognize this?

8 A. Yes.

9 Q. What do you recognize it to be?

10 A. It is just what I said, a table of the infected
11 computers with the location, with their opt sign, which
12 is like how long they have been connected to the
13 internet, their estimated internet speed, version of the
14 software, so this was 000, so it means it was the first
15 version.

16 Q. Of what software?

17 A. Of the Trojan.

18 Q. So looking at sort of the pink column, what is
19 that?

20 A. Which one?

21 Q. The pink column marked IP.

22 A. That's the IP of the infected computer, and with the
23 last digits are the open port so you could connect.

24 Q. And what is the green column entitled "relay"?

25 A. Some of the infected computers you couldn't connect

Mr. Tiberiu Danet - Direct

1 to them directly. There is a list of the ones you could
2 connect directly, but some of them — and the IP is the
3 same as the relay in all of them.

4 In some of them, you had to connect through
5 another computer, and that was called a relay. But
6 again, this is a list of — there is no such infected
7 computer here.

8 Q. Okay. Where would the relay be in relation to the
9 central computer and the infected computer?

10 A. The relay — the relay proxy server would be again
11 one of the infected computers, but like I said, for some
12 infected computers, it would be a difference. If you
13 wanted to connect to an infected computer, sometimes you
14 could do it directly; sometimes you had to go through
15 another infected computer. That was the relay.

16 Q. Okay. So the communication between an infected
17 computer and the central sometimes went through a
18 relay?

19 A. Yes.

20 Q. It was not always a straight direct line.

21 A. Yes.

22 Q. What was the purpose of that?

23 A. Well, this was coded by Nicolescu, but I know that
24 some computers you could just not with the firewalls and
25 everything, some infected computers you couldn't open a

Mr. Tiberiu Danet - Direct

1 port just to connect to them, so you needed to do this
2 bypass through another computer.

3 Q. Okay. Then, can you tell us, what's the next column
4 entitled "action"?

5 A. The P was a ping to the infected computer, and it
6 would check if it is online.

7 Q. Okay.

8 A. DH was something that helped you connect through a
9 relay. If you clicked it, it would display another
10 field, and I am afraid to say I don't know what the A
11 is.

12 Q. And what is the host column?

13 A. The host column is just the — every IP has a host
14 name.

15 Q. Now, can you tell looking at Exhibit 1446-2 where
16 the command or the central server is located?

17 A. If you look at the address bar, it has got the
18 IP 6720514206.

19 Q. And what is that?

20 A. It is an IP address. It is a server. It is a
21 computer located online.

22 Q. And this is an example of the web page interface?

23 MR. O'SHEA: Object.

24 THE COURT: Sustained.

25

Mr. Tiberiu Danet - Direct

1 BY MR. BROWN:

2 Q. You designed this?

3 A. Yes.

4 Q. And this is a web interface?

5 MR. O'SHEA: Object.

6 THE COURT: Sustained.

7 BY MR. BROWN:

8 Q. Were there other types of .PHP files on the central
9 computer, on the central server? I'm sorry.

10 A. Yes, a lot.

11 Q. What types of .PHP files were on the central
12 server?

13 A. You mean names or —

14 Q. Functions.

15 A. For example, I don't remember each name, what the
16 file was, whatever file, but there was one there for
17 each. The Trojan computer would connect to some domain
18 names at first to get its initial information, and you
19 could — that was called HSD.PHP, and you could change
20 those domain names from the interface, but there were
21 tens of pages like that. It was very complex.

22 Q. Did the — what purpose did the .PHP pages serve for
23 the Trojan?

24 A. Two purposes: One was a page such as this that
25 would help us see information about the network, and

Mr. Tiberiu Danet - Direct

1 another type of file was the files that the computer
2 would connect to to get information from the server.

3 Q. Okay. And what kind of file was that?

4 A. What do you mean?

5 Q. Like what type of file?

6 A. .PHP file.

7 Q. .PHP file?

8 A. Yes.

9 Q. And what types of functions did those .PHP files
10 perform?

11 A. For example, each computer had a list of arrivals,
12 key and name. For example, city and state, the ones
13 shown here were actually arrivals.

14 So there was an update to say that it was
15 called fire .PHP, and that would be displayed for a
16 specific IP, all the arrivals.

17 Q. And what was the purpose of having that information
18 on the central server?

19 A. This information had to be stored somewhere because
20 it couldn't be stored on the infected computers.

21 Q. Why not?

22 A. Because there was things saved on the infected
23 computer, too, but you have to have a server to control
24 the whole array of computers. You have to have something
25 with a database where you put on the information you get

Mr. Tiberiu Danet - Direct

1 from the computers and from which you managed the
2 botnet.

3 Q. You mentioned a botnet. What is a botnet?

4 A. A botnet is a collection of a network of computers,
5 a network of bots, infected computers.

6 Q. And who controls the botnet?

7 A. Whoever has access to the central server.

8 Q. Did the four people, including yourself, have a
9 central computer or central server?

10 MR. GOLDBERG: Objection.

11 THE COURT: Overruled.

12 A. No. There is one central server.

13 Q. For your group?

14 A. Yes.

15 Q. And did that central server control a botnet?

16 A. Yes.

17 Q. Why did your group have a botnet.

18 A. Well, it evolved to be a botnet from something else.

19 Initially, it was not a botnet. Like when you say
20 "botnet," you think about — you think about
21 functionality such as the one I previously mentioned.

22 MR. GOLDBERG: Objection.

23 THE COURT: Sustained.

24 BY MR. BROWN:

25 Q. Initially what was — you said initially it was not

Mr. Tiberiu Danet - Direct

1 a botnet?

2 A. Yes.

3 Q. Initially what was it?

4 A. Initially is what I first mentioned. It was
5 just something that would be eBay pages on people's
6 computers.

7 Q. When did it become a botnet?

8 A. At the end of — actually, in 2014, around that.

9 Q. And —

10 A. Or before that, but it was solely a botnet like
11 there was no eBay scheme involved after 2013.

12 Q. So what happened in 2013 to change your group's
13 behavior from eBay to a botnet?

14 A. It was a multitude of reasons. One of them was, it
15 became harder to maintain the eBay scheme. I personally
16 didn't want to do that no more. I was over like — I had
17 done it too long. I was overtricking people to sell them
18 cars.

19 Q. Let me stop you.

20 Why did it become too hard in 2013 to do the
21 eBay scheme?

22 A. It was more difficult for one to list things on
23 eBay, to list the cars on eBay. That was one of the
24 reasons.

25 Q. Why?

Mr. Tiberiu Danet - Direct

1 A. Because of eBay's procedures, they would just
2 identify like not illegal but auctions, such as the ones
3 we posted, and they would take them down almost
4 immediately, so it was not effective.

5 Q. The fraudulent part?

6 A. Yes.

7 Q. And what else happened in 2013 to change the Trojan
8 from an eBay fraud to a botnet?

9 A. Well, I was again in 2013, for example, I had a
10 surgery. So I was not online for about three months or
11 four months. When I came back in 2014, Nicolescu and
12 someone else were already working towards just building a
13 botnet instead of doing the eBay scheme.

14 Q. Did you join them in their efforts?

15 A. Eventually, I did.

16 Q. Why?

17 A. This for me, it became something that was more
18 technological oriented than what happened before, and it
19 was just getting a lot of information, sorting and
20 something that challenged me, the technology from a tech
21 point.

22 Q. What kind of information was the botnet collecting
23 at that point?

24 A. Credit card information, log-ins such as e-mail
25 log-ins, gmail log-ins, Yahoo log-ins, eBay. Then even

Mr. Tiberiu Danet - Direct

1 web history.

2 Q. How was it collecting the credit card information,
3 the log-in information, and those other types of
4 information?

5 A. I explained it previously with the Facebook example.
6 For example, you could make a computer display. When the
7 user went to e-mail instead of displaying the authentic
8 gmail page to display a fake e-mail page, and the user
9 was then transferred to the central command server and
10 saved.

11 Q. So it was presenting fake credential pages?

12 A. Yes.

13 Q. How was it doing that?

14 A. Nicolescu called them injections. It was just a
15 list of domain names that were intercepted and displaying
16 fake pages.

17 Q. And once that web page was injected, it could
18 collect or it looked like a real page?

19 A. It looked exactly like a real page.

20 Q. And a user would type in their information?

21 A. Yes.

22 Q. And what would happen with that information?

23 A. It would be saved.

24 Q. It would be what?

25 A. Saved.

Mr. Tiberiu Danet - Direct

1 Q. Saved?

2 A. Yes.

3 Q. Where?

4 A. On the central server.

5 Q. And how many injections, how much information was
6 coming in daily?

7 A. Depends whether you wanted to collect one day, you
8 would send this request to the infected computers to
9 collect gmail information, and you could get it that day
10 or the following day you would even tens of —

11 Q. Tens of thousands of —

12 A. Yeah, or 10,000, I would say 10,000.

13 Q. Of credentials?

14 A. Yes, 10.

15 MR. GOLDBERG: Objection.

16 THE COURT: Sustained.

17 BY MR. BROWN:

18 Q. Was that information when you received it on the
19 central server organized by hand.

20 A. No. It was — you needed additional software to go
21 through it, parse it, sort it, and so on.

22 Q. And who wrote that software?

23 A. I did.

24 Q. And how could that information be sorted?

25 A. You need certain algorithms. The log-in was not the

Mr. Tiberiu Danet - Direct

1 most difficult part. A lot of information was received
2 from people's web history, and that was really hard to
3 sort because it was huge.

4 Q. So you were also collecting web history?

5 A. Yes.

6 Q. What do you mean by web history?

7 A. Pages that people went to, like just the addresses,
8 not images or anything like that.

9 Q. How did the botnet or Trojan know to collect web
10 history?

11 A. It is a modified version of Firefox, a web browser
12 that was installed in place of the normal Firefox
13 software.

14 Q. So in addition to these injection web pages, it
15 would inject a fake Firefox?

16 A. Yeah. It would just uninstall their Firefox browser
17 and install another one that was exactly the same only
18 had this additional function.

19 Q. And what is Firefox again?

20 A. A web browser just like Internet Explorer, anything
21 used to access the website.

22 Q. So the Trojan could create a fake Firefox?

23 MR. GOLDBERG: Objection.

24 THE COURT: Sustained.

25

Mr. Tiberiu Danet - Direct

1 BY MR. BROWN:

2 Q. It injected a Firefox?

3 MR. GOLDBERG: Objection.

4 THE COURT: Sustained.

5 BY MR. BROWN:

6 Q. And when that web history came back, what happened
7 with that information?

8 A. That could be parts for again, for a user name
9 because that's sometimes available in web history or for
10 giving credit cards, but there was a lot of work to do
11 that because the amount of information received from so
12 many computers, that was totally huge.

13 Q. And how was that information processed?

14 A. Through certain software running on the central
15 server.

16 Q. And who created that software?

17 A. I did. Nicolescu helped me a little bit.

18 Q. What about your background made it possible for you
19 to write that software?

20 A. I would say mostly the algorithmic knowledge that I
21 gained during my high school and college years.

22 Q. Are these databases?

23 A. No. This is a database right there. (Indicating.)

24 Q. Pardon me?

25 A. This is a database. (Indicating.)

Mr. Tiberiu Danet - Direct

1 Q. Would information be put in databases?

2 A. Yes.

3 Q. What's the benefit of putting large amounts of data
4 in databases?

5 A. You can continue to store and search through them.
6 You can very easily search for information.

7 Q. Now, once you collected data through all
8 these various methods, were those computers still
9 infected?

10 A. Yes.

11 Q. Were they still part of the botnet?

12 A. Yes.

13 Q. What would you do with the botnet in addition to
14 collecting information, if anything?

15 A. Starting in 2014, there was cryptomining of
16 cryptocurrency. Some of the computers, not all,
17 would mine cryptocurrency. They used their power to
18 processing power to earn cryptocurrency such as bitcoin
19 or others.

20 Q. And what's the benefit of using a botnet in
21 cryptomining?

22 A. Because instead of using one computer, processing
23 one computer is processing power or better said, the more
24 power you have, the more cryptocurrency you win by
25 mining. So by joining the power of thousands of

Mr. Tiberiu Danet - Direct

1 computers or tens of thousands of computers, you have a
2 really, depending on the cryptocurrency, you have a
3 higher chance of gaining something.

4 Q. By the time of your arrest, how many bots were in
5 your botnet?

6 A. More than a hundred thousand.

7 Q. Okay. And were you making money from cryptomining?

8 A. Yes. But that didn't start when cryptomining
9 started; this started later.

10 MR. GOLDBERG: Objection.

11 THE COURT: Sustained.

12 BY MR. BROWN:

13 Q. At that time, were you still using amightysa to
14 communicate criminally with members of your group —

15 MR. O'SHEA: Objection.

16 Q. — at the time of your arrest?

17 A. Yes.

18 THE COURT: Overruled.

19 Q. And approximately how many people at the time of
20 your arrest were in your group?

21 A. At least four.

22 Q. Four?

23 A. Yes.

24 Q. And how many of those group of four were writing
25 programs to support the botnet?

Mr. Tiberiu Danet - Direct

1 MR. GOLDBERG: Objection.

2 THE COURT: Overruled. How many, if any?

3 THE WITNESS: Two.

4 BY MR. BROWN:

5 Q. How many, if any, were involved in the daily
6 maintenance of the botnet?

7 A. Three.

8 Q. Now, I would like to direct your attention to
9 Government's Exhibit 367.

10 THE COURT: You do not want the jurors to
11 see it?

12 MR. BROWN: Not yet. I just want to confirm
13 my handwriting is correct.

14 BY MR. BROWN:

15 Q. Do you recognize this?

16 A. Yes. It is the part of the chat communications on
17 my home Jabber chat server.

18 Q. Is this what you called a criminal Jabber?

19 MR. GOLDBERG: Objection.

20 THE COURT: Sustained.

21 Q. Is — does this contain hundreds of Jabber chats?

22 MR. GOLDBERG: Objection.

23 THE COURT: Sustained.

24 BY MR. BROWN:

25 Q. Is this a compilation of your — all of your

Mr. Tiberiu Danet - Direct

1 chats?

2 MR. O'SHEA: Objection.

3 THE COURT: Sustained.

4 BY MR. BROWN:

5 Q. Have you reviewed this document?

6 A. Yes.

7 Q. Does it contain a copy of your Jabber chats?

8 MR. O'SHEA: Object.

9 MR. GOLDBERG: Objection.

10 THE COURT: Sustained.

11 BY MR. BROWN:

12 Q. What is it?

13 A. It is a table of some, not all, the communications
14 that went through this server. Actually, it is — I
15 think there is — it contains just my communications. If
16 you go to the other pages, I could —

17 Q. From what you reviewed, is it a fair representation
18 of your chat logs?

19 A. Yes.

20 Q. Okay. And this is in a format that is easy for you
21 to review?

22 A. Yes. It is from, to, and the message from the
23 computer.

24 Q. If I could have you look at page 667 —

25 MR. BROWN: Could I show this to the jury,

Mr. Tiberiu Danet - Direct

1 your Honor?

2 MR. GOLDBERG: Objection.

3 MR. O'SHEA: Objection. Which pages?

4 (Discussion off the record.)

5 MR. O'SHEA: Let's do them one at a time.

6 MR. BROWN: This will be 667.

7 MR. GOLDBERG: Objection.

8 THE COURT: One moment.

9 MR. GOLDBERG: May we approach?

10 THE COURT: Yes. Mr. Brown, I didn't hear
11 what you just said.

12 MR. BROWN: I have line numbers for the
13 pages.

14 THE COURT: Okay. But you want to
15 specifically publish 667?

16 Mr. Goldberg, you are objecting?

17 MR. GOLDBERG: I am.

18 THE COURT: All right. Side bar.

19 (Side bar held on the record.)

20 THE COURT: Sue, would you go back to 667
21 for me? I'm sorry. Okay.

22 MR. BROWN: Your Honor, these are
23 communications between co-conspirators between Danet and
24 Miclaus and Nicolescu. I will be pulling up specific
25 lines.

Mr. Tiberiu Danet - Direct

1 MR. GOLDBERG: The exhibit is not just
2 between co-conspirators but a bunch of other people, too,
3 and he said when he looked at it, he could only identify
4 it as some but not all of the communications on the
5 Jabber server.

6 And then, you said, was this a very accurate
7 copy of these messages, and he said yes, but it is really
8 not because it doesn't include everything; it is just
9 what the Government cherrypicked.

10 THE COURT: Well, do you have the entire —

11 MR. GOLDBERG: I am sure that we have in the
12 disclosures the entire Jabber chat.

13 THE COURT: Right. So it is your position
14 that you want this witness to view them all and to say
15 that they are all fair and accurate and then have the
16 Government cherrypick?

17 MR. GOLDBERG: It is my position that this
18 is more leading of the witness by showing him an exhibit
19 that just is part of a much larger file that just
20 contains certain conversations.

21 Also, it is not limited to just the criminal
22 conspiracy. There is lots of extraneous statements and
23 conversations in the exhibit as well. That's 700 pages
24 long, your Honor.

25 THE COURT: Okay. But the Government at

Mr. Tiberiu Danet - Direct

1 this point is asking only to publish this particular
2 page.

3 MR. BROWN: I have several pages and several
4 lines within the pages. So we can highlight or zoom in
5 on specific lines.

6 THE COURT: Okay. And you have communicated
7 those pages and lines to defense counsel?

8 MR. BROWN: I just did, your Honor.

9 MR. GOLDBERG: You identified a 700-page
10 exhibit, and now we are going to pull out a few pages
11 from that, and that was identified last night. But I
12 think what counsel is about to say, we know what's
13 relevant to this case in these chats. It is not like it
14 is a mystery.

15 I know what pages he is going to. It is a
16 large exhibit. If he goes to the pages, which are going
17 to be conversations between the witness and allegedly my
18 client — I don't think between him and Mr. O'Shea's
19 client — but my client and the witness, so I know
20 about those, but this was a large exhibit identified last
21 night.

22 THE COURT: But I apologize, Mr. Goldberg.
23 I am confused here. The Government is going to point out
24 conversation between this witness and your client.

25 MR. GOLDBERG: I am assuming.

Mr. Tiberiu Danet - Direct

1 THE COURT: Please tell me the basis for
2 your objection.

3 MR. GOLDBERG: The basis for my original
4 objection?

5 THE COURT: No, no.

6 MR. GOLDBERG: I don't have an objection —

7 THE COURT: Do you have an objection to the
8 Government showing him conversation between you and —
9 between the witness and your client.

10 MR. GOLDBERG: Not a good one.

11 THE COURT: Okay. So I will allow you to
12 point out conversation between this witness and his
13 client.

14 MR. BROWN: Yes, your Honor.

15 THE COURT: All right. And do you have any
16 further conversation you want out?

17 MR. BROWN: In this exhibit, no. However,
18 we have e-mail addresses that have been testified to with
19 just subject lines and occasionally an attachment with
20 e-mail addresses that have been, I believe, all
21 identified in his testimony.

22 THE COURT: So specifically as to
23 Mr. Goldberg's client.

24 MR. BROWN: Yes, your Honor.

25 THE COURT: Any objection to those?

Mr. Tiberiu Danet - Direct

1 MR. GOLDBERG: No, not on the basis —

2 THE COURT: As to Mr. O'Shea's client?

3 MR. BROWN: Correct, your Honor, same for
4 him.

5 THE COURT: Any objection?

6 MR. O'SHEA: Here is what I suggest.

7 How many pages of that exhibit are we
8 talking about, Duncan?

9 MR. BROWN: Seven or eight.

10 MR. O'SHEA: In order to move it along
11 before they are published to the jury, show them, and I
12 will say objection. And you can make a ruling based on
13 the side bar, and I am preserved for the record.

14 My objection would be constant insinuation
15 that it is Nicolescu or Miclaus in the form of the
16 question is unfair to the facts. All they have is what
17 they call monikers or e-mail addresses.

18 I don't have a problem saying this is to
19 this e-mail address, but to name these people as an
20 assumed fact is an improper question in my opinion.

21 THE COURT: You have to have the witness
22 identify who the conversation is between. And again,
23 watch the leading.

24 MR. BROWN: I will, your Honor.

25 (Side bar concluded.)

Mr. Tiberiu Danet - Direct

1 THE COURT: For the record, very specific as
2 to what you would like Mr. Goldberg and Mr. O'Shea to
3 look at.

4 MR. BROWN: Yes, your Honor.

5 If we could pull up the page, before
6 publishing to the jury, page 668, line 114 and 99.

7 THE COURT: 11 —

8 MR. BROWN: 4, 99.

9 THE COURT: 99. Okay. Mr. Goldberg, do you
10 see it? Ms. Chandler, you are unable to isolate it?

11 MS. CHANDLER: Correct.

12 THE COURT: Then we will not publish it to
13 the jury. However, you can have testimony regarding
14 it.

15 Why don't we just have testimony? We will
16 do it the old fashioned way when I started in the
17 business.

18 BY MR. BROWN:

19 Q. What is — what was your Jabber handle?

20 A. Romeo and Romeo Mobile.

21 Q. And what was the difference between those two?

22 A. The first one I was using from my laptop; the second
23 one from my phone.

24 Q. And did you have communications with Defendant
25 Nicolescu over Jabber?

Mr. Tiberiu Danet - Direct

1 A. Yes.

2 Q. What did you know his Jabber name to be?

3 A. Obe and Obe Mobile.

4 Q. Okay. Did you know any other names?

5 A. On the Jabber server?

6 Q. Yes.

7 A. No.

8 Q. Could we close that?

9 Could you pull up Government's Exhibit 1852
10 without publishing to the jury first? Looking at 1852,
11 what is this?

12 A. It is a list of e-mails sent from my e-mail
13 account.

14 Q. And did you review this document prior to Court?

15 A. Yes.

16 Q. And is this an accurate representation of
17 e-mails from between March 22nd, 2013, and August 15th,
18 2014?

19 A. Yes.

20 Q. And again, what is your e-mail address in this
21 exhibit?

22 A. Amightysa@gmail.com.

23 Q. And what e-mail address did you know Bogdan
24 Nicolescu to be?

25 A. Master Fraud at GMX.com.

Mr. Tiberiu Danet - Direct

1 Q. And I don't think we have done this yet.

2 Do you see Bogdan Nicolescu in Court
3 today?

4 A. Yes.

5 Q. Could you point him out and describe what he is
6 wearing?

7 A. Gentleman with the glasses wearing a blue shirt.

8 Q. Does he have a tie on?

9 A. No.

10 Q. Does he have a suit?

11 A. Yes.

12 Q. What color?

13 A. Dark blue or black. I can't see.

14 MR. BROWN: Can the record reflect the
15 witness identified Bogdan Nicolescu?

16 THE COURT: Front table or back table?

17 THE WITNESS: Front table.

18 THE COURT: Record may so reflect.

19 BY MR. BROWN:

20 Q. In our looking at April 19, 2013, do you see that
21 line? I'm sorry —

22 A. April 2014?

23 Q. Do you see April 19, 2014, do you see that?

24 A. Yes.

25 Q. And do you see there is also an e-mail for a

Mr. Tiberiu Danet - Direct

1 Minolta 9797?

2 MR. O'SHEA: Objection to the form.

3 THE COURT: Sustained.

4 BY MR. BROWN:

5 Q. Do you see at the bottom e-mail or second from the
6 bottom who is that e-mail involving?

7 A. The second from the bottom?

8 Q. Yes.

9 A. Minolta 9797 at GMX.com?

10 Q. Yes.

11 A. Minolta 9797 was the handle of Miclaus.

12 Q. And do you see — do you know his full name?

13 A. Yes, Radu Miclaus.

14 Q. And do you see Radu Miclaus in Court today?

15 A. Yes.

16 Q. Could you point him out and describe what he is
17 wearing?

18 A. He is the Defendant in the back table, blue — light
19 blue shirt.

20 Q. Does he have a suit?

21 A. Yes.

22 Q. And does he have a tie?

23 A. No.

24 Q. Does he have any glasses?

25 A. No.

Mr. Tiberiu Danet - Direct

1 MR. BROWN: Could the record reflect the
2 witness pointed out Miclaus?

3 THE COURT: Record may so reflect.

4 MR. BROWN: Thank you.

5 BY MR. BROWN:

6 Q. And actually, the middle e-mail, what is the subject
7 of that?

8 A. Yahoo hosting, you mean, the middle, yes,
9 yeah.

10 Q. What is the subject line?

11 A. Yahoo hosting.

12 Q. And does that mean anything to you?

13 A. Yes.

14 Q. What does that mean to you?

15 A. At one point, we needed to create a lot of the Yahoo
16 domain names that it bought from Yahoo, and it became so
17 cumbersome that we — that I made kind of a tool that
18 would help you create them instead of doing it by hand,
19 like going through the process, choosing a user name,
20 putting in the credit card information.

21 This tool would help you create it faster by
22 just putting all the information in one page, and it
23 would create the domain name.

24 Q. And looking at the bottom entry, do you recognize
25 that e-mail?

Mr. Tiberiu Danet - Direct

1 A. All the .PHP?

2 Q. Yes. And what, if anything, does that mean?

3 A. Yes. That was one of the .PHP pages I mentioned
4 that was located on the control server, that basically
5 contained mostly everything to communicate with the
6 infected computers.

7 Q. Now, if we can look at March 5th, 2014. Okay. Do
8 you recognize the middle e-mail 5:28:34?

9 A. It is an e-mail that has a name with the name Casper
10 d-e-p-s-r-a-r, which is an archive of files.

11 Q. And what is .PGP, what does that mean to you?

12 A. .PGP, the attachment was encrypted using the key to
13 .PGP. .PGP stands for creating good privacy. It is a
14 software.

15 Q. Okay. And what is Casper if you know?

16 A. Casper is also a software.

17 Q. And what does Casper do?

18 A. It enables you to control a web browser like
19 clicking, virtually clicking buttons, entering
20 information into a browser without actually having to do
21 it by hand.

22 Q. Okay. And what is d-e-p or d-e-p-s?

23 A. It was short for dependencies.

24 Q. And what's that?

25 A. What's called a dependency, something that a program

Mr. Tiberiu Danet - Direct

1 relied on. If it needed certain files to work, that
2 would be a dependency.

3 Q. And is that something that's commercially available,
4 the dependency program.

5 A. It is commonly used.

6 Q. The software that was — I will withdraw that
7 question.

8 Could we look at 24 June 2013, page 1?

9 MR. O'SHEA: Which page?

10 MR. BROWN: 24 June 2013.

11 THE COURT: Are we in the same exhibit?

12 MR. BROWN: Yes, your Honor, we are.

13 BY MR. BROWN:

14 Q. Okay. And could you look at the line for the middle
15 24 June 2013?

16 A. Yes.

17 Q. Okay. And who is that to?

18 A. Ra101Putin, was another one of my brother's e-mail
19 addresses. The second one is Master Fraud, Nicolescu.

20 Q. And what's the subject line of that?

21 A. "How to spam."

22 Q. Okay. And what, if anything, did that mean to
23 you?

24 A. It was spam, means sending unsolicited e-mails to a
25 lot of addresses. Probably everyone that has an e-mail

Mr. Tiberiu Danet - Direct

1 receives spam, a lot of spam messages. This was a guide
2 how to use the botnet to send such e-mails.

3 Q. Now, looking at June 24, 2014, and do you recognize
4 that line?

5 A. Yes.

6 MS. CHANDLER: This is July?

7 Q. And who is that from?

8 A. It is from Nicolescu to me.

9 Q. And what is the subject matter?

10 A. Polon.

11 Q. And what does that mean to you?

12 A. It is short for Polonex, which is a website that
13 allows you to change, to exchange one cryptocurrency for
14 another.

15 Q. Okay. And if we go up to June 14th — June 16th, do
16 you recognize this e-mail?

17 A. Yes.

18 Q. And who is that between?

19 A. It is from Nicolescu to Miclaus and me.

20 Q. And what is the subject?

21 A. "Bitcoin exchange."

22 Q. And what is the attachment?

23 A. The attachment is archive. That contains a
24 multitude of files, more than one file. And by the
25 name of it, it contains accounts for bitcoin exchange

Mr. Tiberiu Danet - Direct

1 websites.

2 Q. Okay. At this point with your group — or was the
3 group doing bitcoin mining?

4 A. Yes. But without much success.

5 Q. And did these e-mails discuss the bitcoin mining?

6 A. Yes.

7 MR. GOLDBERG: Objection.

8 THE COURT: Sustained.

9 BY MR. BROWN:

10 Q. Now, if we could pull up Exhibit 1851 without
11 publishing to the jury, do you recognize this?

12 A. The whole page?

13 Q. Yeah. Have you reviewed 1851, Exhibit 1851?

14 A. Yes, I have.

15 Q. Do you recognize it?

16 A. Yes.

17 Q. What do you recognize it to be?

18 A. The same thing, a list of e-mails sent between me
19 and others.

20 Q. Okay. Now, could we look — could we highlight
21 2 December 2014? Do you recognize the e-mail on December
22 2nd, 2014?

23 A. Yes.

24 Q. And —

25 MR. BROWN: Could we publish this at this

Mr. Tiberiu Danet - Direct

1 point?

2 BY MR. BROWN:

3 Q. What is the subject line?

4 A. E-mailing, and that's the name of a file, lib p-f-f.

5 Q. What is L-i-b-p-f-f?

6 A. L-i-b-p-f-f is a public library that allows you to
7 extract e-mails from the Outlook account, from a computer
8 that has Outlook installed.

9 THE COURT: The jurors are not seeing this,
10 Mr. Brown.

11 MR. BROWN: I thought they were seeing
12 this.

13 THE COURT: No, not based upon —

14 MR. BROWN: I thought I asked to publish
15 it.

16 THE COURT: But based on our conversation
17 over at side bar, I don't know where we are at with this
18 issue. Side bar.

19 (Side bar held off the record.)

20 THE COURT: So Mr. Goldberg, you are not
21 objecting to this being published?

22 MR. GOLDBERG: I am not. Go ahead.

23 THE COURT: Mr. O'Shea, the same?

24 MR. O'SHEA: Same.

25 THE COURT: And yet, Mr. O'Shea, you are

Mr. Tiberiu Danet - Direct

1 reserving your right to argue admissibility.

2 MR. O'SHEA: Yes, ma'am.

3 THE COURT: All right.

4 MR. BROWN: Your Honor, could we have a
5 five-minute break to figure out a computer problem.

6 THE COURT: Sure. All rise for the jury.
7 Short recess, folks.

8 (Recess had.)

9 THE COURT: Please be seated. You may
10 continue.

11 MR. BROWN: Thank you.

12 BY MR. BROWN:

13 Q. Can you please take a look at Exhibit 367? Do you
14 recall these? Do you know what these are?

15 A. Yes.

16 Q. What are they?

17 A. They are chats from my mobile.

18 Q. And to whom are they sent or between?

19 A. Between me and Nicolescu.

20 Q. And again, what is your moniker here?

21 A. Romeo-Mobile.

22 Q. Okay. And what does that -Mobile mean?

23 A. That it is the account that I used on my phone.

24 Q. Looking at — looking at line 26579, could you read
25 what the subject line say?

Mr. Tiberiu Danet - Direct

1 A. In English, "well, you do the JS."

2 Q. And what, if anything, does that mean to you?

3 A. Actually, the translation is more like, well, you
4 pass the JS." JS is —

5 MR. GOLDBERG: Objection.

6 THE COURT: Sustained.

7 BY MR. BROWN:

8 Q. Do you know what JS means?

9 A. JavaScript.

10 Q. And what's that?

11 A. It is a programming language.

12 Q. And was that programming language used by the
13 group?

14 A. Yes, a lot.

15 MR. GOLDBERG: Objection.

16 THE COURT: That's all right. Overruled.

17 BY MR. BROWN:

18 Q. What was the purpose of using JavaScript?

19 A. JavaScript has to do with the web pages, modifying
20 the web pages, that sort of thing. Here, in particular,
21 it is what is used to program the virtual processor, the
22 one that I said you don't need to type or move the mouse.
23 You just do it using code.

24 Q. Okay. And could you look at line 26577? What's the
25 subject of that?

Mr. Tiberiu Danet - Direct

1 A. But I'm saying when you run the plug-in —

2 Q. And what does that mean?

3 A. There were several plug-ins ran on the —

4 MR. GOLDBERG: Objection.

5 THE COURT: Was there an objection?

6 MR. GOLDBERG: Objection, your Honor.

7 THE COURT: I didn't hear it. Overruled.

8 A. There were several plug-ins to run by the infected
9 computers.

10 Q. Okay. And I apologize, is that a subject line, or
11 what did I just have you read?

12 A. It is a chat message.

13 Q. Okay. But called a chat subject line?

14 A. Yeah.

15 Q. And is that you responding to obe?

16 MR. GOLDBERG: Objection.

17 THE COURT: Sustained.

18 BY MR. BROWN:

19 Q. Do you know who typed — but I'm saying when you run
20 the plug-in?

21 MR. GOLDBERG: Objection.

22 THE COURT: Overruled. Do you know, sir?

23 THE WITNESS: Yes.

24 BY MR. BROWN:

25 Q. Who was it?

Mr. Tiberiu Danet - Direct

1 A. Me, because the lines that started in upper case
2 character come from my phone, because I had the setting
3 when you type on your phone, it capitalizes your first
4 character.

5 Q. And can we go to page 716? And could you look at
6 line 26530?

7 A. Yes.

8 Q. And what is that chat?

9 A. A miner force.

10 Q. What did that mean to you, if anything?

11 A. This was a file located on the server that would
12 mine cryptocurrency.

13 Q. Did it do anything else?

14 A. No, but it mined different cryptocurrencies, not
15 just one.

16 Q. And when you say "on the server," what do you mean
17 by that?

18 A. On the central server, on that what was connected to
19 the botnet.

20 Q. Okay. Now, could you look at 26532, and what does
21 it say?

22 A. It says run pipe s-t-d-i-n.

23 Q. And what, if anything, does that mean to you?

24 A. Apart from a typo, be instead of end run pipe,
25 s-t-d-i-n something contained in the code.

Mr. Tiberiu Danet - Direct

1 Q. And, in fact, 26538, could you read that?

2 A. "And I run with run pipe."

3 Q. Does that refer to the line you just read?

4 A. Yes.

5 Q. Now, if we could look at page 717, and could you
6 look at 26555, and what does that say?

7 A. Yes.

8 Q. And what does that say?

9 A. "Doesn't that d-e-p depends on JS."

10 Q. And what is a d-e-p, what does that mean to you, if
11 anything?

12 A. It is short for dependence.

13 Q. And if you look at 26560, what does that say?

14 A. "When you do that .exe.d-e-p.

15 Q. And what is a .e-x-e.d-e-p if you know.

16 A. It is part of the file name contained by all the
17 plug-ins on the central computer server.

18 Q. And is a d-e-p a file you used with this group?

19 A. Yes. It is a name that is held on.

20 MR. GOLDBERG: Objection.

21 THE COURT: Overruled.

22 BY MR. BROWN:

23 Q. And is this actually an extension?

24 MR. GOLDBERG: Objection.

25 Q. Or what is it?

Mr. Tiberiu Danet - Direct

1 THE COURT: Sustained.

2 BY MR. BROWN:

3 Q. Okay. What form does the file take?

4 A. For example, .e-x-e.d-e-p is an encrypted executable
5 file.

6 Q. And if you look at line 26567, could you read that?

7 A. "For every JS."

8 Q. And again, what does JS mean to you, if anything?

9 A. JavaScript.

10 Q. And do you know what that chat was about or that
11 comment was about?

12 A. The whole conversation is about how to run —

13 MR. GOLDBERG: Objection.

14 THE COURT: Sustained.

15 BY MR. BROWN:

16 Q. Okay. Could we please take a look at page 732?
17 Could we look at line 26941. Could you read that,
18 please?

19 A. "I see that it's still extracting something."

20 Q. And what does that mean to you, if anything?

21 A. It means that there are still new e-mails
22 being extracted for them to be sent from infected
23 computers.

24 Q. And if you look at 26943, could you read that?

25 A. "And s-q-l."

Mr. Tiberiu Danet - Direct

1 Q. And what, if anything, does s-q-l mean to you?

2 A. S-q-l is a database format and software.

3 Q. Is that a database you are familiar with?

4 A. Yes. It is the database we used on the central
5 server.

6 Q. And what did you use that database for?

7 A. To store everything related to the botnet.

8 Q. Okay.

9 A. Every data.

10 Q. And if you look at line 26946 —

11 A. Yes.

12 Q. Could you read that?

13 A. "With epoll."

14 Q. And what does that mean to you?

15 A. Epoll was something that Nicolescu made was on the
16 server, and it had to do with relaying the proxy servers.
17 I don't have any more details, but it is something that
18 was used on the server.

19 Q. And if you could look at line 26947, and could you
20 read that?

21 A. The one that constantly gave a ping.

22 Q. And what, if anything, does that mean to you?

23 A. It means that there was something that constantly
24 sent a signal, a signal to the server.

25 Q. Can we look at page 733 and look at line 26966? I'm

Mr. Tiberiu Danet - Direct

1 sorry, I transposed my handwriting.

2 Could we look at 26981? All right. And
3 what does that say?

4 A. "And I think the power is more important anyway."

5 Q. Okay. What, if anything, does that mean to you?

6 A. It means that Nicolescu considered power more
7 important than anything else, I suppose, such as
8 mine.

9 Q. If we look back up to 26972, can you read that?

10 A. "This way the VPS will work."

11 Q. And what does "VPS" mean to you?

12 A. The virtual private server. It is a server that you
13 buy.

14 Q. And if you look at line 26973?

15 A. Yes. It says "up to a hundred K."

16 Q. And what, if anything, does that mean?

17 A. A hundred K means 100,000, and those two lines
18 combined means that the server, that the central server
19 will hold up to a hundred thousand infected computers
20 maintaining 100,000 infected computers.

21 Q. Okay. And if you look at the next line 26974, what
22 does that say?

23 A. "Without problem."

24 Q. And what does that mean?

25 A. That it will hold without problem up to 100,000

Mr. Tiberiu Danet - Direct

1 computers.

2 Q. And if you look at line 26978, could you read that?

3 A. "Now we really have power."

4 Q. Okay. And is that — do you know if that's to you
5 or from you?

6 A. It is to me.

7 Q. Okay. And who is it from?

8 A. Nicolescu.

9 Q. Couple questions: How would you access the central
10 server?

11 A. You need a user name and password and connect to
12 that using the user name.

13 Q. How many people that you knew of had user names and
14 passwords for the central server?

15 A. That I knew of three. It changed during the course
16 of time, so it depends on the —

17 Q. At the height, how many at the most?

18 A. Probably more than three or four.

19 Q. Okay. And who were those four?

20 A. Nicolescu, me, Miclaus, sometimes Linx when he was
21 — so another person when he was around. That's what I
22 am aware of. There could be others.

23 Q. Nobody else?

24 A. That I know of, no.

25 Q. Now, was there just one central server?

Mr. Tiberiu Danet - Direct

1 A. Yes. It was one server, and whenever it would go
2 down because of — I don't — say credit card errors
3 because this server was — they took it down because the
4 credit card doesn't work any more. It would be set up
5 somewhere else and copied. The information was being
6 copied. So its location has been changed by, but the
7 content was the same.

8 Q. When you go to the central server, did it look like
9 a regular desktop?

10 MR. GOLDBERG: Objection.

11 THE COURT: Overruled.

12 A. No. It is a screen just containing text.

13 Q. How would you know when you are on the central
14 server where to go?

15 A. Because I knew the structure of the folders, the
16 files.

17 Q. Was there an internal structure on the central
18 server?

19 A. Yes. There were folders, different folders, and
20 subfolders. Everything had a structure.

21 Q. Could we take a look before publishing to the jury
22 at Exhibit 2203?

23 THE COURT: Before publishing?

24 MR. BROWN: Yes. I just want to confirm
25 with the witness. 2203.

Mr. Tiberiu Danet - Direct

1 BY MR. BROWN:

2 Q. Do you recognize this?

3 A. Yes. It is —

4 Q. What is it?

5 A. It is a part of this structure of a sub sub sub sub
6 folder.

7 Q. And is it a fair and accurate representation of a
8 substructure?

9 A. Yes.

10 Q. And do you recognize the description on the top of
11 the page?

12 A. Yes.

13 Q. Was that on the central server?

14 A. Yes, it is on the central server.

15 MR. BROWN: And can I publish this to the
16 jury?

17 MR. GOLDBERG: No objection?

18 MR. O'SHEA: No objection.

19 BY MR. BROWN:

20 Q. Could you describe to the jury what 2203 is?

21 A. It is a list of folders and inner folders, and they
22 contain files about structure. Each of the names, links,
23 MF was actually a user, one of us or one of the
24 nicknames.

25 Q. Okay. And is this a directory?

Mr. Tiberiu Danet - Direct

1 MR. GOLDBERG: Objection.

2 A. Yes.

3 THE COURT: Sustained.

4 BY MR. BROWN:

5 Q. What is this?

6 A. It is a directory and subdirectories.

7 Q. Okay. What does a directory do?

8 A. It holds files for other directories.

9 Q. And what does a subdirectory do?

10 A. The same thing. They can be nasty.

11 Like a directory can contain other
12 directories, too, and those directories can contain
13 directories, too, up to —

14 Q. Like a file cabinet that holds files?

15 MR. O'SHEA: Objection.

16 THE COURT: Sustained.

17 BY MR. BROWN:

18 Q. Is what you are looking at a subdirectory?

19 A. Yes. It is a subdirectory of the directory listed
20 on top.

21 Q. What is the directory listed on top?

22 A. Well, there is more, Phantom JS flash work space, so
23 the subdirectory is called "work space."

24 Q. And what is a work space? What does that mean to
25 you?

Mr. Tiberiu Danet - Direct

1 A. In this case, it contains files about — for each
2 user, it contains files necessary for things like the
3 Yahoo subdirectory of Amy; would contain files maybe to
4 create Yahoo domain names by the user Amy and so on.

5 Q. And who is Amy?

6 A. It was short for amightysa, so that's me.

7 Q. And who is Linx?

8 A. Linx is Dima Catalin.

9 Q. And who are or is MF?

10 A. MF is Nicolescu.

11 Q. And who is Min?

12 MR. O'SHEA: Objection.

13 THE COURT: Overruled.

14 A. M-i-n is short for Minolta. It is Miclaus.

15 Q. And who is natiune, n-a-t-i-u-n-e?

16 A. It is pronounced natinue meaning nation. It is a
17 person that was brought into this by Miclaus, but I never
18 knew.

19 MR. GOLDBERG: Objection.

20 Q. Do you know the name of that?

21 THE COURT: One moment. Overruled. But do
22 a follow-up.

23 BY MR. BROWN:

24 Q. Do you know who that nickname —

25 A. No. I only know the nickname.

Mr. Tiberiu Danet - Direct

1 Q. And who is next?

2 A. Raul.

3 Q. Do you know who Raul is?

4 A. Yes, that's my brother.

5 Q. And who is next?

6 A. Sasha, I have no idea.

7 Q. And do you know who is next?

8 A. T-r-x. Again, I have no idea.

9 Q. And who are the next four?

10 A. User 1, 2, 3, 4, I don't know, but they look like
11 test directories, but I don't know.

12 Q. Is this part of the central server that is password
13 protected?

14 A. Yes.

15 Q. You can only get to this part with the password
16 user?

17 A. Yes. You need a credential.

18 MR. GOLDBERG: Objection.

19 THE COURT: Sustained.

20 BY MR. BROWN:

21 Q. And do you know if the AOL and Yahoo, were those
22 files used in the botnet?

23 A. They were used for creating quicker accounts with
24 those services instead of doing it manually.

25 Q. Could we look at finally Exhibit 380?

Mr. Tiberiu Danet - Direct

1 THE COURT: I'm sorry. 380?

2 MR. BROWN: 3-8-0, yes.

3 BY MR. BROWN:

4 Q. And do you recognize this?

5 A. Yes. It is another list of chat messages between my
6 Mobile phone and my user account and Nicolescu.

7 Q. Okay. And is it a fair and accurate copy of your
8 chat —

9 MR. GOLDBERG: Objection.

10 Q. — of your phone?

11 MR. GOLDBERG: Objection.

12 THE COURT: Start over and ask your
13 question, please.

14 BY MR. BROWN:

15 Q. Do you recognize this?

16 A. Yeah.

17 Q. What is it?

18 A. It is a list of chat messages between me and
19 Nicolescu.

20 Q. Okay. What is it?

21 A. A list of chat messages between my phone and
22 Nicolescu.

23 Q. Is it a fair and accurate representation of chat
24 messages between those two phones?

25 A. Yes.

Mr. Tiberiu Danet - Direct

1 Q. Okay. And could you please zoom in on the third and
2 fourth lines? Okay.

3 And looking at the middle line, could you
4 read what that says?

5 A. It says "I have one card LOL. LOL I took one card
6 from 20K e-mails."

7 Q. Okay. And what, if anything does that mean to
8 you?

9 A. That out of 20,000 e-mails sent to people, one card
10 was the wrong credit card information was obtained.

11 Q. Okay. Could you read the next line?

12 A. "Uh-huh, the bad ones, Vanghelie.

13 Q. Okay. And what, if anything, does that mean to
14 you?

15 A. Vanghelie was a file, Vanghelie.txt was a file
16 containing credit cards on the server.

17 Q. And what kind of credit cards, if you know, did it
18 contain?

19 A. Excuse me?

20 Q. On what server was the Vanghelie?

21 A. The central server.

22 Q. Okay. And do you know where the credit cards it
23 contained came from?

24 A. Spam e-mail.

25 Q. Okay. And were those spams sent by the

1 botnet?

2 A. Yes.

3 Q. As part of the botnet scam?

4 A. Yes.

5 MR. GOLDBERG: Objection.

6 THE COURT: Sustained.

7 BY MR. BROWN:

8 Q. And who named the file Vanghelie?

9 A. Nicolescu did. Vanghelie is the name of a mayor in
10 Romania known for his stupidity.

11 MR. BROWN: No further questions. Thank
12 you, your Honor.

13 THE COURT: Ladies and gentlemen, we are
14 going to adjourn for the evening.

15 Now, I know people have been asking Mary
16 approximately when the trial will be concluded. During
17 voir dire, I indicated that we anticipated this being a
18 two, two and-a-half week trial. I can represent to you
19 that we are on target; we are on schedule.

20 So we do anticipate that the case will be in
21 your hands at approximately a little less than the two
22 and-a-half week mark. But this case is not over.

23 Do not discuss it amongst yourselves or with
24 anyone else. Do not form any opinion regarding this
25 matter. Please be downstairs at 9:00 a.m. tomorrow. We

1 will call for you and bring you up as a group.

2 Have a good evening. All rise for the jury.

3 (Jury out.)

4 THE COURT: Okay, folks. Please be seated.

5 Let's go over the exhibits for the day, and
6 consistent with what we have done in the past, I will
7 simply state the number and assume that it is being
8 offered and assume there is no objection unless you tell
9 me to the contrary.

10 And if I am going too fast, you let me know.

11 Not —

12 MR. O'SHEA: Judge — I'm sorry.

13 THE COURT: That's all right.

14 MR. O'SHEA: Before we begin this — and I
15 know we do this with extreme efficiency — having said
16 that, I already said at side bar that it can be one
17 exhibit, but we will slow down when we —

18 THE COURT: Yes, definitely. I marked it
19 down.

20 MR. O'SHEA: Thank you, Judge.

21 THE COURT: 1907, 1901, 1903, 1248, 1421,
22 2105, 2107, 2108, 1, 65, 2041.

23 MR. GOLDBERG: Could we see 65?

24 THE COURT: Sure.

25 MS. CHANDLER: I believe 65 was a physical

1 exhibit on the cart.

2 THE COURT: 65 is the Samsung phone.

3 MR. GOLDBERG: Okay.

4 THE COURT: 2041.

5 MR. McDONOUGH: Acer laptop.

6 THE COURT: 2042.

7 MR. McDONOUGH: Laptop.

8 THE COURT: 2003.

9 MR. McDONOUGH: Samsung hard drive.

10 THE COURT: 2046.

11 MR. McDONOUGH: Router.

12 THE COURT: 2040, desktop.

13 MS. CHANDLER: That must be the HP desktop.

14 MR. BROWN: HP desktop.

15 THE COURT: 2038, 2039, 5.

16 MS. CHANDLER: That's the one I got.

17 THE COURT: 2045.

18 MR. O'SHEA: Yes, objection to 5, only as
19 references to my client, which we could probably get by
20 redaction. I think if we scroll down there is references
21 to my client saying that this is his.

22 MS. CHANDLER: I assume you want the English
23 version.

24 THE COURT: You know, folks, we need to be
25 careful because everything is on the record here. If you

1 want to have a private conversation, just say so, and
2 then George will not put it on the record.

3 MR. O'SHEA: I don't have — I am fine with
4 doing this on the record myself. Michael, I don't know
5 about you.

6 MR. GOLDBERG: Yeah, I —

7 THE COURT: You are asking, Mr. O'Shea,
8 you are asking that any reference to your client be
9 redacted?

10 MR. O'SHEA: Yes.

11 THE COURT: Government?

12 MR. BROWN: Yeah, we object.

13 MR. O'SHEA: Here is the thing. If I am not
14 mistaken, this was — is this the search of Danet's
15 place?

16 MR. GOLDBERG: It is the search of
17 Nicolescu's place.

18 MR. O'SHEA: My client wasn't there. They
19 didn't interview my client there and talk to him there,
20 and they are just referencing things there. It is all
21 hearsay. There is no foundation placed for how his name
22 got there or anything else nor any testimony.

23 THE COURT: You wanted to speak,
24 Mr. Goldberg?

25 MR. GOLDBERG: Yeah. I would object just to

1 the record in and of itself. It is a legal document,
2 search warrant, inventory. I don't think it has any
3 independent evidentiary value, and it is translated in a
4 foreign language.

5 I think whatever probative value it would
6 have would be outweighed by unfair prejudice. So I would
7 object to search warrant and the return being put in
8 evidence at all.

9 MR. LEVINE: So this is not search warrant,
10 your Honor. This is just the inventory taken in the
11 house. We separately marked the search warrant, but we
12 did not introduce it.

13 I heard an objection to the fact it is a
14 foreign document that has been translated, but we have a
15 stipulation as to the accuracy of the translation. I
16 heard a 403 prejudice objection. I don't see this as
17 really prejudicial.

18 It is just a list of what was found in the
19 house. The agent who was there during the search
20 testified as to the circumstances under which this was
21 obtained. So I don't think it is objectionable, your
22 Honor.

23 THE COURT: Specifically, there is an
24 objection of hearsay, and I believe Mr. O'Shea is
25 indicating that the only way any items can be identified

1 as being his client's is through hearsay.

2 MR. LEVINE: So we addressed this in our
3 hearsay motion, and we can address it now —

4 THE COURT: I don't believe — correct me if
5 I am wrong — I don't believe I granted a motion pretrial
6 allowing this exhibit into evidence.

7 MR. LEVINE: No. But that's why I am
8 addressing it now.

9 To the extent that the only person who could
10 have indicated that it was the item belonged to Miclaus
11 rather than Nicolescu, that would be the statement of the
12 opposing party, and that would be the statement of
13 Nicolescu.

14 THE COURT: Wait a minute. I am to assume
15 Nicolescu told the agents at the home that this
16 particular item belongs to Miclaus?

17 MR. LEVINE: In fact, if you look at the
18 items listed there, they are bank cards that have — I
19 mean, you have to look at the individual statements.

20 THE COURT: But that's why I am turning to
21 you because, let me tell you, the objection is based on
22 hearsay. And I cannot assume that a co-Defendant said
23 "this was Miclaus' item." So you need to go through item
24 by item and convince me that it is not based on hearsay.

25 MR. O'SHEA: Judge, in fairness to them

1 there are some items that they found that are listed
2 there that have my client's name on them. So I get that,
3 and I might be confused — and this might be my fault,
4 there was another — it looks like search warrant return
5 that we went over with one of the witnesses.

6 I think the forensic guy that came in
7 today, that lists items that are referenced as being my
8 client.

9 THE COURT: Look it, if you are going to
10 object, we need to go through item by item because I do
11 not accept the argument that the prejudicial effect
12 outweighs the probative value. I do not accept that, the
13 authentication argument.

14 The only argument I am considering is the
15 hearsay argument. Therefore, we have to go through item
16 by item and determine if we have a hearsay problem.
17 So —

18 MR. BROWN: Your Honor, I believe the
19 reference by Miclaus — and I just did a quick scan — I
20 believe the reference to Miclaus is that at some point he
21 and Nicolescu rented the apartment. It looks like there
22 is an attribution of Nicolescu items found in X room or
23 Y room. It doesn't say this is Miclaus' backpack or this
24 is —

25 THE COURT: Let me say it again.

1 MR. LEVINE: Why don't we take this offline,
2 and Mr. O'Shea will look at the specific lines and which
3 ones are prejudicial.

4 THE COURT: That's fine.
5 2045.

6 MR. O'SHEA: That's what I was talking
7 about, same thing. We will go over that the same way.

8 THE COURT: I will hold 2045 back.
9 1874, is that demonstrative only, or are you
10 offering it?

11 MR. LEVINE: Yes. We are offering that,
12 your Honor.

13 MR. BROWN: Yes, we are offering it, your
14 Honor.

15 MR. GOLDBERG: Is it substantive evidence.
16 I don't have a problem with this being shown to
17 explain the testimony during the course of a trial,
18 during argument, but as a substantive exhibit, I would
19 object.

20 MR. O'SHEA: And here is my supplement to
21 what Michael just said, Judge, and that is that the
22 witness himself was even kind of sketchy about what it
23 all meant. I don't think the witness even provided
24 enough foundation assuming it could be admitted.

25 THE COURT: 1874 will not be admitted into

1 evidence. This is not the type of, quote unquote,
2 summary as envisioned by our rules. That's purely a
3 demonstrative piece of evidence. But certainly, you can
4 use it during questioning of further witnesses and during
5 closing argument.

6 1415, are you offering that?

7 MS. CHANDLER: The directional antenna.

8 MR. GOLDBERG: I object to the directional
9 antenna. I think he was talking about it in general. He
10 identified it. He said it was a directional antenna, but
11 if it was seized from one of the Defendants, there needs
12 to be more foundation.

13 MR. BROWN: We will provide another witness
14 tomorrow.

15 THE COURT: So you are not offering it at
16 this time?

17 MR. BROWN: No, your Honor.

18 THE COURT: All right. Now, we have the
19 exhibits that were the subject of side bar conferences.

20 So let me group them. 367, 1852, 1851, 2203
21 and 380.

22 MR. O'SHEA: 3-8-0, Judge?

23 THE COURT: 380.

24 MR. O'SHEA: I just didn't hear you.

25 THE COURT: So 367.

1 MR. BROWN: 367, your Honor, we would be
2 offering 715, 716, 717, 732, 733, 734.

3 THE COURT: Could you slow down just a
4 bit?

5 MR. BROWN: Absolutely.

6 THE COURT: 715 to 717?

7 MR. BROWN: Yes.

8 THE COURT: 732 to 7 —

9 MR. BROWN: -34.

10 THE COURT: 734.

11 MR. BROWN: Yes.

12 MR. GOLDBERG: Those are Jabber chats.

13 MR. BROWN: Yes.

14 THE COURT: Whenever you are ready,

15 Mr. Goldberg.

16 MR. GOLDBERG: I am not objecting.

17 THE COURT: Mr. O'Shea?

18 MR. O'SHEA: I am objecting and here is why.

19 It is in itself native format. This thing, as I
20 understand it, is a cellphone from Danet's phone at the
21 Miami airport. Am I correct?

22 THE COURT: Is that Government?

23 MR. McDONOUGH: Yes, yes.

24 THE COURT: Go ahead.

25 MR. O'SHEA: I think Agent Macfarlane will

1 be able to describe this better than this witness. This
2 was a chart created by a program from a phone dump.

3 THE COURT: You want to wait until all of
4 the witnesses have testified before addressing this?

5 MR. O'SHEA: Yes.

6 THE COURT: Any problem with that?

7 MR. BROWN: We can do that, your Honor.

8 THE COURT: All right. Same with 1852 or
9 I'm sorry, I should ask you, first, Mr. Brown what are
10 you offering in 1852?

11 MR. BROWN: Well, 1852 these are e-mails —

12 THE COURT: Are you offering the entire
13 exhibit?

14 MR. BROWN: Yes.

15 THE COURT: Any objection, Mr. Goldberg?

16 MR. GOLDBERG: Well, I don't think it has
17 been properly — I don't think a foundation has been laid
18 for this yet because this also came from a phone dump,
19 correct?

20 THE COURT: Do you want to wait?

21 MR. GOLDBERG: Mr. Danet said yes, these are
22 my e-mails, but we don't have the actual source of this
23 exhibit.

24 THE COURT: Do you want to wait, Government?

25 MR. BROWN: No, your Honor. These were

1 provided in search warrants, which have been certified.

2 MR. GOLDBERG: These were taken from the
3 search warrants, from the command control server?

4 MR. LEVINE: Search warrants from Google.

5 MR. GOLDBERG: And we stipulated to that.

6 MR. BROWN: Yes.

7 THE COURT: No objection?

8 MR. GOLDBERG: I am better with it. I
9 thought they were just coming in — I wouldn't object.

10 THE COURT: Mr. O'Shea?

11 MR. O'SHEA: You are offering the whole
12 exhibit, the whole document, guys?

13 MR. BROWN: Yeah, yes.

14 MR. O'SHEA: I have to look, Judge. There
15 are references in here. They are offering the document,
16 so this document is the report that you got from Google
17 when you issued a search warrant to gmail for gmail
18 transmissions?

19 MR. BROWN: Yes, correct.

20 MR. O'SHEA: And it just has the to and
21 from, the subject matter of the e-mail but obviously not
22 the content of the e-mail?

23 MR. LEVINE: Content was all encrypted.

24 MR. O'SHEA: And this saves Google coming in
25 having to — they would be able to authenticate it

1 anyway. All right. No objection.

2 THE COURT: 1851, are you offering?

3 MR. BROWN: Yes, your Honor.

4 THE COURT: Mr. Goldberg?

5 MR. GOLDBERG: Same thing. From a Google
6 search warrant?

7 MR. BROWN: Yes.

8 MR. GOLDBERG: No objection.

9 MR. O'SHEA: What's the difference between
10 1851 and 1852?

11 MR. BROWN: It came from different search
12 warrants.

13 MR. GOLDBERG: 1852, Master Fraud was the —

14 MR. BROWN: No.

15 MR. O'SHEA: 1852 the from e-mail is from
16 amightysa, from Master Fraud. There are a number of
17 different froms.

18 MR. BROWN: And multiple search warrants.

19 MR. O'SHEA: As long as it was obtained from
20 gmail, same way, different search warrants, guys?

21 MR. BROWN: Yes.

22 MR. O'SHEA: Then I can't object.

23 THE COURT: All right. 2203?

24 MR. BROWN: We are offering that, your
25 Honor.

1 MR. GOLDBERG: What is it?

2 MR. BROWN: The command and control
3 directory.

4 MR. GOLDBERG: 2203.

5 MR. O'SHEA: That's that little Daisy chain
6 or whatever it is?

7 MR. BROWN: This is from the search warrant.

8 MR. GOLDBERG: No objection.

9 MR. O'SHEA: 2203 is — how did you guys get
10 this again because he couldn't tell you.

11 MR. BROWN: They send us a CD of the server,
12 and we print it out, the directory, and it is a copy of
13 the directory.

14 MR. O'SHEA: Was this directory in what they
15 sent or something you guys created?

16 MR. LEVINE: This was within the site file.

17 MR. O'SHEA: Tell me what you mean by that.
18 I mean because Brian can probably clear this up when he
19 testifies.

20 MR. BROWN: And he will testify about
21 multiple directories. It is 44 directories. The whole
22 directory can be 28, 30 pages long.

23 MR. GOLDBERG: This is a work space
24 directory.

25 THE COURT: Let's go off the record

1 because —

2 (Discussion held off the record.)

3 THE COURT: All right. 380?

4 MR. BROWN: Offering, your Honor. Same as
5 367; same theory.

6 MR. O'SHEA: 380 is what?

7 MR. BROWN: Is Jabber.

8 THE COURT: We are holding off on 367?

9 MR. BROWN: We can hold off on this one.

10 THE COURT: We can hold off as well. On
11 behalf of the Government, did I miss any?

12 MR. BROWN: I don't think so, your Honor.

13 THE COURT: All right. We are in
14 adjournment. Thank you, sir.

15 (Trial adjourned at 5:10 p.m.)

16 — — — — —

17 C E R T I F I C A T E

18 I, George J. Staiduhar, Official Court
19 Reporter in and for the United States District Court,
20 for the Northern District of Ohio, Eastern Division,
21 do hereby certify that the foregoing is a true
22 and correct transcript of the proceedings herein.

23

24 s/George J. Staiduhar
25 George J. Staiduhar,